Ministerie van Defensie

Beleidsvisie

Informatiegestuurd Optreden

sneller slimmer sterker

Versie 1.3

Inhoud

Samenvatting

Strategische context

Defensie streeft ernaar wereldwijd militaire operaties slimmer, sneller en sterker uit te kunnen voeren. Daarvoor is het belangrijk om conflicten beter te begrijpen en dat te benutten *(to outsmart the enemy)*. IGO moet Defensie in staat stellen informatiedominantie[1] te verkrijgen in zowel de fysieke, virtuele en cognitieve dimensie. Hiervoor moet informatie, inclusief inlichtingen op maat, tijdig en op alle niveaus beschikbaar zijn. Dit stelt eisen aan de organisatie en haar processen. Het vermogen om onze omgeving goed te beschrijven (*insight*) en veranderingen aan te zien komen (*foresight*), moet zich continu ontwikkelen en aanpassen aan de veranderende omgeving.

Meer informatie legt een steeds grotere druk op de mogelijkheden van het Inlichtingen- en Veiligheidssysteem van Defensie om de besluitvormer van het gewenste omgevingsbeeld te voorzien, ook waar het om de signaalfunctie gaat (*indicators & warnings*). Het is daarom van belang dat op alle niveaus over voldoende capaciteiten wordt beschikt, zodat relevante inlichtingen tijdig beschikbaar zijn voor de commandovoering op alle niveaus (het gestuurd optreden).

Een belangrijk kenmerk van IGO is dat de inlichtingen sneller horizontaal, verticaal en lateraal door de militaire domeinen en organisatie moet kunnen worden verspreid. De complexe, vaak hybride omgeving vraagt om snelle en duidelijke synchronisatie van de beschikbare tijd, het militair vermogen, de gegunde gevechtsruimte en de kwaliteit van de informatie. IGO betekent niet zozeer dat iedereen altijd alle gegevens deelt. Dat hangt immers af van de hoofdtaak, de context van de inzet[2] en de juridische grondslag. IGO betekent dat alle krijgsmachtdelen snel en zorgvuldig met elkaar en met bondgenoten relevante informatie moeten kunnen delen, onder alle omstandigheden, wanneer de inzet dat verlangt.

Informatiegestuurd Optreden

Informatie Gestuurd Optreden (IGO) houdt in dat Defensie in staat is:

1. (Informatie) sneller de juiste informatie verzamelen en analyseren teneinde de situatie beter te begrijpen, zodat
2. (Gestuurd) snellere en betere besluiten genomen kunnen worden, om
3. (Optreden) met de beschikbare (militaire) middelen de gewenste effecten te bereiken.

Daartoe bevat IGO drie bouwstenen.

- **Informatie als doel:** informatie als bron voor het inlichtingenproces, ten behoeve van *forecasting* (voorspellend vermogen), *insight* (voor beeldvorming), en *foresight* (voor oordeelsvorming), die samen het benodigde begrip van de operatieomgeving opleveren.

[1] Informatiedominantie: het initiatief en controle houden over onze operationele omgeving door snel en veilig informatie te kunnen delen tussen de verschillende domeinen en besluitvormingsniveaus om daarmee de dynamische aard van het moderne conflict bij te kunnen benen.

[2] Zie “type operaties”, paragraaf 2.4

- **Informatie als middel:** informatie ter ondersteuning van de commandovoering, voor effectieve besluitvorming en bevelvoering, zowel voor de gereedstelling als de inzet van de krijgsmacht.
- **Informatie als effector:** informatie waarmee effecten in de fysieke, cognitieve en virtuele dimensie kunnen worden bereikt, in een synergetische combinatie met kinetische middelen.

Denken in dimensies

Het dimensiemodel is een manier van denken om domein-onafhankelijk potentiële effecten en afhankelijkheden van militaire activiteiten binnen de operationele omgeving te duiden. Daarmee zorgt het voor een integrale benadering voor het bereiken van doelstellingen zonder daarbij in de valkuil van een 'single-domain' benadering te stappen.
Het raamwerk wordt gevormd door drie dimensies: fysiek, virtueel en cognitief. De effecten in deze dimensies zijn uiteindelijk gericht op het (veranderen van) gedrag. In de cognitieve dimensie worden percepties gevormd en besluiten genomen met het oog op de (beïnvloeding van) besluitvorming. Alle dimensies zijn met elkaar verbonden en beïnvloeden elkaar.

- **De cognitieve dimensie.** Deze dimensie gaat over het beïnvloeden van de wil (emoties, overtuigingen, waarden, percepties, (voor)oordelen, belangen en doelstellingen van individuen en organisaties en omvat alle vormen van onderlinge interactie).
- **De virtuele dimensie.** Deze dimensie gaat over niet-tastbare communicatie van data, informatie, inlichtingen en kennis zoals tekst en beelden, stuurgegevens, protocollen. Deze niet-tastbare communicatie maakt doorgaans gebruik van cyberspace en het elektromagnetische spectrum.
- **De fysieke dimensie.** Deze dimensie gaat over alle zichtbare en tastbare elementen die informatie communiceren en/of bij zich dragen, evenals hun geografische locatie, zoals fysieke objecten (satellieten, routers en gebruikersapparatuur, voertuigen en (wapen) platformen), infrastructuur (communicatienetwerken) en de mens als fysiek persoon (als lichaam).

Randvoorwaarden

Om Informatiegestuurd Optreden succesvol te kunnen toepassen is een aantal randvoorwaarden van belang.

Juridische en ethische kaders

Kunnen, willen en mogen; om gezien de continue en snel veranderende dreigingen de grondwettelijke taken van de krijgsmacht uit te kunnen blijven voeren, zal Defensie samen met belanghebbende partijen (zowel binnen als buiten Defensie) voortdurend moeten blijven verkennen en testen hoe er binnen de bestaande juridische en ethische kaders effectief gehandeld kan en mag worden. Als willen en mogen niet langer in evenwicht te brengen zijn, zal ook verkend moeten worden of de wetgeving herijkt dient te worden om Nederland te mogen beschermen voor de continue en snel veranderende dreigingen in het informatiedomein. De mandaten die binnen en buiten de defensieorganisatie afgegeven kunnen en mogen worden om met gegevens en informatie te werken zijn een randvoorwaarde om informatiegestuurd op te treden.[3]

[3] Zie ook: Nota algemene juridische kaders voor activiteiten van de krijgsmacht in de informatie-omgeving, BS2021006577, 12 April 2021.

Robuustheid en weerbaarheid

Defensie dient haar eigen IT- en wapensystemen tegen cyberaanvallen te beschermen (*cyber resiliency*). Dit maakt deel uit van haar eigen digitale weerbaarheid. Daarnaast dient Defensie redundantie (back-up systemen) in te bouwen voor Defensie IT en wapensystemen, hieronder valt ook informatie *resiliency*: de mate van redundantie waarin informatie via verschillende wegen tot je kan komen (fysieke dimensie, informatiedragers). Ook zal Defensie nauw samen moeten werken met de aanbieders van vitale processen en aan de bescherming daarvan moeten (kunnen) bijdragen wanneer Nederland zelf overgaat tot offensieve cyberoperaties, waarbij repercussies op die processen waarschijnlijk zijn.

IGO data ontsluiting, connectiviteit en interoperabiliteit bij grote projecten

De koppeling tussen IGO en grote materieelprojecten spitst zich toe op de kernvraag: "In hoeverre houdt Defensie bij de verwerving van groot materieel – en breder gezien bij het ontwikkelen van capaciteiten – rekening met IGO?" Aspecten die daarbij van belang zijn, zijn onder andere principes als *privacy en security by design en default*, zeggenschap over gegevens, interoperabiliteit, connectiviteit, *data-labeling* en filtering, dataverzameling en –ontsluiting en cybersecurity. Deze moeten nog nadrukkelijker in scope en budget van de programma's en/of projecten geadresseerd worden. Hierbij geldt dat het niet alleen moet gaan om het platform zelf, maar ook om de (informatie)omgeving waarin dat platform moet opereren.

Samenwerken

De ontwikkelingen op het gebied van IGO gaan razendsnel, waardoor Defensie niet in alle gevallen in staat is om alles zelf te doen. Meer dan ooit kijkt Defensie naar kennisinstellingen, industrie, NAVO/EU partners voor samenwerking en het benutten van reeds ontwikkelde oplossingen. Zowel de Strategische Kennis en Innovatie Agenda[4] als de Defensie Industrie Strategie[5] zetten in op een weloverwegen balans tussen het volgen van civiele ontwikkelingen en het ontwikkelingen van militaire toepassingen in samenwerking met onze private partners.

Datamanagement en *data governance*[6]

De defensieonderdelen kennen ieder hun eigen dynamiek en behoeven hun eigen aanpak om invulling te geven aan het Informatiegestuurd optreden met behulp van data. Er is echter een aantal gemeenschappelijke uitdagingen die om een integrale aanpak vragen: geschikte technologische voorzieningen, inzicht in de manier waarop *data science* en AI impact zullen hebben op de werkzaamheden en vaardigheden van onze medewerkers en data management en *governance*. Naast technologische mogelijkheden, is een goed uitgewerkte, breed gedragen en ingerichte *data governance* een belangrijke randvoorwaarde voor het behalen van onze ambities. Defensie heeft de taken, verantwoordelijkheden en bevoegdheden op dit vlak vastgelegd en werkt momenteel aan de professionalisering hiervan.

Security by design[7]

Bij de ontwikkeling van *data science* en AI-toepassingen is beveiliging een integraal en belangrijk onderdeel van het ontwerpproces (*security-by-design* principe) om kwetsbaarheden in de systemen te voorkomen. Daarbij dient rekening gehouden te worden met data-beveiliging en rubricering waarbij het koppelen van systemen voor bepaalde toepassingen nieuwe vraagstukken met zich mee brengt. Er zal binnen de juridische- en ethische kaders per situatie gekeken moeten worden naar de te beschermen belangen op het gebied van veiligheid, privacy en praktische bruikbaarheid.

[4] Defensie Strategische Kennis- en Innovatieagenda (SKIA) 2021-2025, november 2020
[5] Defensie Industrie Strategie (DIS), november 2018
[6] Zie ook Defensie Strategie Data Science en AI.
[7] Zie ook Defensie Strategie Data Science en AI.

Privacy by design
Wet- en regelgeving stelt specifieke eisen aan de verwerking van persoonsgegevens zodat het grondrecht van privacy wordt beschermd. Volgens de Algemene Verordening Gegevensbescherming (AVG) moet de verwerking van persoonsgegevens voldoen aan beginselen van:
- Rechtmatig, zorgvuldig en transparant
- Doelbinding (welbepaald, uitdrukkelijk omschreven en gerechtvaardigd)
- Minimale gegevensverwerking
- Juistheid
- Opslagbeperking
- Integriteit en vertrouwelijkheid (passende technische en organisatorische maatregelen)
- Verantwoordingsplicht

Doorontwikkeling

Naast het feit dat deze beleidsvisie een gemeenschappelijke (conceptuele) basis biedt voor het actualiseren van (deel)strategieën en andere beleidsproducten, is deze visie tevens de basis voor het verder concretiseren van de doelstellingen en ontwikkelen van de hiervoor benodigde capaciteiten. Op basis van bovenstaande zijn er zes actielijnen en daarbinnen aanbevelingen voor hoe de IGO transformatie kan worden vormgegeven.

Actielijn 1: Commandovoeringsprocessen en –structuren.
Een nieuwe commandostructuur zal op alle niveaus van oorlogvoering (strategisch, operationeel en tactisch) moeten voorzien in adequaat orkestrerend vermogen dat zich kan aanpassen aan de verschillende contexten in de operationele omgeving, waarbij het uitgangspunt is dat verantwoordelijkheid wordt belegd bij die node in het netwerk die de beste *situational understanding* van de omgeving heeft. Het uitgangspunt daarbij is opdrachtgerichte commandovoering, waarbij bevoegdheden naar het laagst mogelijke niveau zijn gemandateerd.

Actielijn 2: Het (fysieke en sociale) netwerk dat sensoren, verwerkings- en analysecapaciteit, commandovoeringselementen en effectoren met elkaar verbindt en de effectoren aanpast aan de veranderingen in de informatieomgeving.
Om de complexe uitdagingen van moderne oorlogvoering het hoofd te kunnen bieden, en daarnaast optimaal gebruik te maken van de mogelijkheden van de digitale transformatie, is een herziening van de manier waarop de diverse entiteiten binnen onze organisatie met elkaar verbonden zijn en samenwerken noodzakelijk. Om optimaal gebruik te maken van de kansen in de informatieomgeving, en voorbereid te zijn op digitale bedreigingen, zal Defensie ook in dit nieuwe domein een gedegen netwerk van sensoren tot en met effectoren (cyberoperaties, elektronische oorlogsvoering en informatieoperaties) moeten creëren om daarmee effectief te zijn in alle dimensies. Deze elementen moeten gekoppeld kunnen worden aan de elementen in de klassieke domeinen zodat er in samenhang gestreefd kan worden naar synergie.

Actielijn 3: De mentaliteit en de manier van werken van het personeel.
IGO is een manier van denken en werken die tot in de haarvaten van de organisatie door moet dringen. De toevoeging van informatiemanoeuvre aan de militaire gereedschapskist noodzaakt aanpassingen aan de manier van het plannen, voorbereiden en uitvoeren van operaties. De conceptuele benadering van informatie als effector zal integraal onderdeel uit gaan maken van onze operationele processen. Het is van belang dat het leiderschap van

Defensie, op alle niveaus, doordrongen is van het belang van deze verandering en deze ook actief uitdraagt. Ook betekent deze verandering dat er meer aandacht moet worden besteed aan juridische en ethische kaders. Naast het optimaal benutten van bestaande wet- en regelgeving is het ook van belang structurele oplossingen op het gebied van wet- en regelgeving verder te verkennen.

Actielijn 4: Een robuuste en veilige IT-infratructuur als fundament voor IGO.
Hoewel IGO veel meer omvat dan de technische component, is een robuuste en veilige IT-infrastructuur inclusief IT-organisatie een noodzakelijke voorwaarde voor het slagen van de IGO-transformatie. Dit IT-fundament moet voorzien in een aantal randvoorwaarden die het mogelijk maken om multi-domein en op alle niveaus van oorlogvoering tijdig en veilig over de juiste informatie te kunnen beschikken. Een aantal aandachtspunten is daarbij van bijzonder belang. Ten eerste moet de IT-infrastructuur informatie en inlichtingen wereldwijd kunnen ontsluiten in zowel de statische als de ontplooide, mobiele en uitgestegen omgeving. Daarnaast zal dit veilig moeten gebeuren, met koppelingen tussen de verschillende rubriceringsniveaus zodat personeel over alle informatie kan beschikken waar zij conform hun rol en veiligheidsmachtiging toegang tot hebben. Verder dient de IT-infrastructuur bestand te zijn tegen verstoringen van technische aard of door acties van een externe actor.

Actielijn 5: Onze connectiviteit en interoperabiliteit met bondgenoten en partners.
In veruit de meeste gevallen zal Nederland niet alleen opereren, maar in bondgenootschappelijk verband, gelegenheidsverbanden (*coalitions of the willing*), of met nationale partners in het veiligheidsdomein. Dit vraagt in de eerste plaats dat het nationale beleid aansluit op bondgenootschappelijke doctrine en concepten. Het uitgangspunt is “NAVO tenzij” wat ertoe moet leiden dat Defensie met dezelfde standaarden werkt om snel en efficiënt met bondgenoten data en informatie te kunnen uitwisselen. In het nationale veiligheidsdomein betekent dit dat Defensie en nationale veiligheidspartners in staat moeten zijn bij nationale inzet geautomatiseerd informatie uit te wisselen om een gedeeld beeld en gezamenlijk begrip van de veiligheidssituatie te kunnen opbouwen teneinde samenwerking met publieke partners te optimaliseren, uiteraard binnen de geldende juridische en ethische kaders.

Actielijn 6: Informatiegestuurd gereedstellen, ondersteunen en besturen.
Informatiegestuurd optreden is alleen effectief als ook de overige hoofdprocessen uit de waardeketen van Defensie (gereedstellen, ondersteunen en besturen) optimaal gebruik maken van inzichten uit data en informatie. Om de hoofdprocessen besturing en ondersteuning verregaand te kunnen ondersteunen met inzichten uit data en informatie is het noodzakelijk dat aan een aantal voorwaarden wordt voldaan. Deze voorwaarden zijn te categoriseren rondom de volgende aandachtsgebieden: organisatie (o.a. capaciteiten, werkwijze, cultuur), processen, data & informatie en technologie.

1 Strategische context en de rol van informatie

Leeswijzer
De Beleidsvisie is als volgt opgebouwd: Hoofdstuk 1 bespreekt de strategische context en de rol die informatie daarin speelt. Hoofdstuk 2 definieert het conceptuele kader van Informatiegestuurd Optreden. Hoofdstuk 3 gaat in op de drie elementen van Informatiegestuurd Optreden, namelijk Informatie Als Doel, Middel en Effector. Hoofdstuk 4 tenslotte identificeert een aantal kritieke randvoorwaarden en schetst een aantal aandachtsgebieden waarbinnen IGO moet worden doorontwikkeld.

1.1 Strategische context

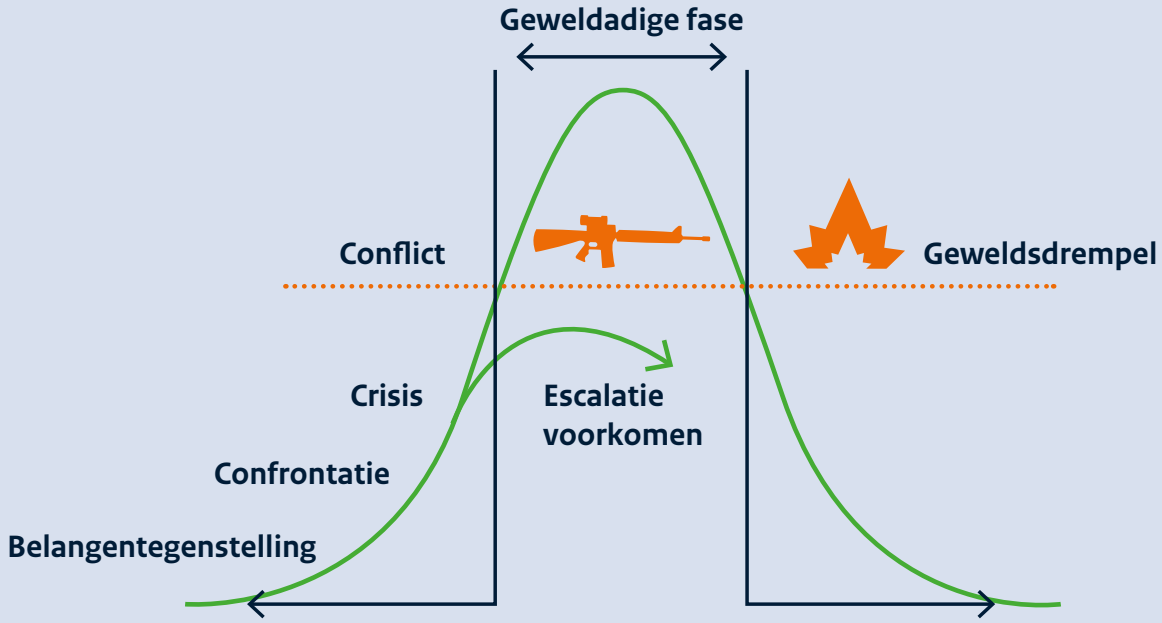
Wereldwijd worden landen geconfronteerd met een scala aan dreigingen. De Russische invasie van Oekraïne is hier een goed voorbeeld van. Op het eerste oog is dat een klassieke oorlog, waar met traditionele slagkracht een gewelddadige strijd wordt gevoerd. Als je echter beter kijkt, wordt duidelijk dat informatie een prominente rol speelt. De snelheid van handelen ligt soms zeer hoog, en de reactietijd is kort. Om dit vol te kunnen houden is de beschikbaarheid van (*near*) *real-time* informatie van groot belang voor effectieve commandovoering. Voor de nieuwe generatie precisie-wapensystemen is accurate en snel beschikbare informatie nodig. Beide partijen gebruiken strategische communicatie om de perceptie van legitimiteit, internationale steun en het eigen moreel te beïnvloeden. Daarnaast zien we dat informatie als effector wordt gebruikt: zowel door de inzet van cybercapaciteiten, maar ook door het veelvuldig gebruik van nieuwe informatietechnologie om desinformatie te verspreiden. Succes is dus niet alleen maar een zaak van voldoende gevechtskracht, maar wordt dus voor een substantieel deel bepaald door het vermogen om te kunnen opereren in die informatieomgeving.

1.2 Aanpassing van Defensie aan veranderende omgeving

Defensie moet kunnen anticiperen op conflicten en speelt een rol bij het voorkomen van escalatie (conflictpreventie). De Veiligheidsstrategie voor het Koninkrijk der Nederlanden ziet verschillende elkaar versterkende dreigingen en thema's, zoals technologische ontwikkelingen en digitalisering, toegenomen afhankelijkheden, grensoverschrijdende ondermijnende criminaliteit, bedreiging van vitale infrastructuur, geopolitieke uitdagingen, militaire, cyber- en hybride dreigingen. Door de toegenomen connectiviteit en complexiteit

kunnen botsende belangen en crises elders sneller een grotere impact hebben op de Nederlandse veiligheid.

Afbeelding 1 laat zien dat een conflict niet uit het niets ontstaat. De krijgsmacht dient voorbereid te zijn op escalatie, niet alleen voor inzet ter bescherming, interventie of stabilisatie, maar juist ook voor een geloofwaardige afschrikking om het zover niet te laten komen. In die zin vervult de krijgsmacht al haar rol nog voordat er sprake is van daadwerkelijke inzet. Informatie is cruciaal om de ontwikkeling van conflicten te kunnen voorzien, duiden, monitoren om de krijgsmacht tijdig gereed te stellen en in een goede uitgangspositie te brengen.



Afbeelding 1: **Conflictpreventie (escalatie voorkomen) en op kunnen treden in de "gewelddadige fase"**[8]

Tijdens inzet opereert de krijgsmacht doorgaans in onvoorspelbare omstandigheden waarin ze zich continu moet aanpassen aan de veranderende omgevingen. Om de juiste besluiten te kunnen nemen en effectief te kunnen optreden is het cruciaal dat we weten wat er om ons heen gebeurt, hoe chaotisch de situatie ook is. Zo moeten we in staat zijn vijandige intenties te begrijpen en aanvallen tijdig te onderkennen, ook al proberen tegenstanders ons te misleiden. Daarbij is het van levensbelang dat we weten waar neutrale partijen of burgers aanwezig zijn. Ook is de inzet van precisiewapens alleen mogelijk met accurate informatie, niet alleen om vijandelijke doelwitten effectief te kunnen aangrijpen maar ook om neven-schade en burgerslachtoffers te voorkomen. Tijdige, relevante en betrouwbare informatie is dus zowel noodzakelijk om missies effectief uit te kunnen voeren, als voor de veiligheid van burgers en eigen troepen.

[8] Ministerie van Defensie, Conflicten Begrijpen, Escalatie Voorkomen, januari 2020.

1.3 Wat verstaan we onder Informatiegestuurd Optreden?

Defensie streeft ernaar wereldwijd militaire operaties slimmer, sneller en sterker uit te kunnen voeren door informatiegestuurd op te treden. Informatie Gestuurd Optreden (IGO) houdt in dat Defensie in staat is:

1. (Informatie) sneller de juiste informatie verzamelen en analyseren teneinde de situatie beter te begrijpen, zodat
2. (Gestuurd) snellere en betere besluiten genomen kunnen worden, om
3. (Optreden) met de beschikbare (militaire) middelen de gewenste effecten te bereiken.

Het gaat hier om:

- binnen de geldende juridische en ethische kaders optimaal gebruik maken van beschikbare informatiebronnen, sensoren en analysecapaciteit;
- uit de toenemende hoeveelheid informatie handelingsopties identificeren om sneller en beter dan de tegenstander besluiten te kunnen nemen;
- een robuust en veilig netwerk om gegevens, informatie en inlichtingen te verwerken en te delen (zowel in de gereedstelling, de operatien als in de ondersteuning), waardoor sensoren, besluitvormers en wapensystemen naadloos kunnen samenwerken;
- het vermogen om kinetische en non-kinetische effecten te sorteren in de fysieke, virtuele en cognitieve dimensie.

Dat moet Defensie in staat stellen zich voortdurend aan te passen aan (1) de veranderende informatieomgeving, (2) de veranderende aard van conflicten en oorlogen, (3) de geopolitieke ontwikkelingen, maar ook (4) de rol die Defensie speelt in het beschermen van vitale infrastructuur.

(1) Aanpassing van Defensie aan een veranderende informatieomgeving

We leven in het informatietijdperk waarbij sprake is van een digitale transformatie. Voor het effectief kunnen benutten van de slagkracht van de krijgsmacht spelen inlichtingen en informatie een cruciale rol. Deze rol heeft aanzienlijk aan belang gewonnen door de enorme toename van de hoeveelheid data en de toename van technologieën zoals kunstmatige intelligentie, *data science*, *cloud computing* en robotisering. De landen die het beste gebruik kunnen maken van de toepassingen hiervan, waaronder de betere ontsluiting en synchronisatiemogelijkheden van informatie maar ook het bewust verspreiden van (des) informatie naar grote groepen, hebben een (strategische) voorsprong en winnen daarmee direct aan (militaire) kracht.

Om te kunnen vechten en te kunnen winnen in, of optimaal gebruik te maken van de informatieomgeving zijn aanpassingen binnen Defensie noodzakelijk. Allereerst moet het militaire besluitvormingsproces van observeren, begrijpen, beslissen, en handelen worden geactualiseerd, door informatie hierin een centralere plaats te geven. Doordat de hoeveelheid informatie en de snelheid waarmee informatie rondgaat blijft toenemen, is het noodzakelijk om bij alle betrokkenen een operationeel beeld te kunnen creëren waarmee ze in het voordeel zijn ten opzichte van hun tegenstander. Om dit succesvol te kunnen toepassen, moet dit in de gereedstellingsfase ook worden geoefend. Omdat oefenen en trainen in die informatieomgeving een wettelijke beperkingen kent[9], zal Defensie moeten investeren in gesimuleerde omgevingen die deze mogelijkheden wel bieden, maar ook moeten verkennen welke mogelijkheden er op het gebied van wet- en regelgeving zijn om gereedstellings-activiteiten op een verantwoorde manier te kunnen uitvoeren.

[9] Onderzoekscommissie Land Information Manoeuvre Centre, “Grondslag gezocht”, december 2022.

Innovaties op het gebied van effectoren en platformen/vectoren creëren nieuwe mogelijkheden voor offensieve, defensieve en stabiliserende activiteiten. Waar Defensie de informatievoorziening de afgelopen decennia als ondersteunend bedrijfsmiddel zag, is deze nu integraal onderdeel van het militair vermogen. De krijgsmacht moet de voordelen van data science en kunstmatige intelligentie succesvoller dan een tegenstander weten te benutten. Hier is in de Strategische Kennis en Innovatieagenda[10] dan ook een prominente plek voor ingericht. Gegevensbeheer, standaardisatie interoperabiliteit, veiligheid, *weerbaarheid* en het daarbij toepassen van principes als *privacy en security by design* van onze informatievoorziening zijn hiervoor nodig.

Onze wapensystemen zijn in toenemende mate in staat om met geavanceerde sensoren zeer grote hoeveelheden aan data te genereren. Dit vereist aandacht in de behoeftestellingsfase bij verwerving voor principes als *privacy en security by design* en zeggenschap over gegevens. De data van de diverse systemen (o.a. F-35, CV-90, onderzeeboten), en de informatie die op basis van deze data wordt geproduceerd, moeten kunnen worden gedeeld met andere eenheden (nationaal en internationationaal). Hiervoor moet een aantal barrières worden weggenomen. Allereerst is onze organisatiecultuur vooral gericht op het afschermen van informatie, maar er is nauwelijks regelgeving of beleid dat het delen van informatie stimuleert, toestaat of zelfs verplicht. Daarbij komt dat de complexiteit van de regelgeving is toegenomen waardoor we te maken hebben met een veelvoud aan juridische en ethische kaders. Veel informatie-bewerkingen zijn bovendien nog handmatig, wat tijdrovend is en de kans op fouten vergroot. Defensie werkt daarom aan duidelijke zeggenschap over gegevens en aan oplossingen om het delen van (gerubriceerde) gegevens en informatie in de praktijk mogelijk te maken.

Defensie moet haar omgang met informatie dus aanpassen. Niet langer meer redeneren vanuit losse organisatie-elementen, maar het optreden benaderen vanuit het concept van multidomein operaties (MDO), waarin synchronisatie van alle activiteiten in de verschillende domeinen centraal staat. Daarnaast moeten we ons aanpassen aan de veranderende en belangrijker wordende informatieomgeving waarin het fysieke domein in toenemende mate een representatie kent in de virtuele dimensie. Daarnaast werkt het optreden in het cyber-domein anders dan het optreden in de fysieke dimensie. Waar we in de fysieke domeinen uitgaan van voldoende tijd om bij een opbouwend conflict tijdig eenheden te formeren en te ontplooien, is het bereik en de dynamiek in het cyberdomein en de informatieomgeving veel groter. Dat noodzaakt om in een eerder stadium een goede uitgangspositie te hebben om handelingsopties voor te bereiden. Het ontwikkelen van een effectief cyberwapen voor een bepaald doel kan maanden of jaren duren.

De mogelijkheden om informatiestromen aan te grijpen en anderen met informatie te beïnvloeden nemen hand over hand toe, zeker met de komst van kunstmatige intelligentie. Daarbij gebeurt het omgekeerde, namelijk dat de informatie in de virtuele dimensie wordt gewijzigd of gemanipuleerd waardoor deze niet meer overeenkomt met de werkelijkheid. (Des)informatie, strategische communicatie, cybersabotage en -spionage leiden tot meer mogelijkheden voor potentiële tegenstanders voor het uitvoeren van hybride campagnes. Daarmee kan ons militair vermogen worden aangetast. Ook onze civiele vitale infrastructuur kan worden aangevallen en onze maatschappij kan grootschalig en langdurig worden ontwricht. (Militaire) operaties in de informatieomgeving zijn een standaard onderdeel van het handelen van onze tegenstanders. De krijgsmacht moet zich aanpassen om de confrontatie met moderne kwalitatief hoogwaardige tegenstanders[11] en sterkere tegenstanders aan te kunnen gaan.

[10] Defensie Strategische Kennis- en Innovatieagenda 2021-2025, december 2020..
[11] Sterkere tegenstanders; zie bv https://www.ft.com/content/f939db9a-40af-4bd1-b67d-10492535f8e0

De snelle ontwikkelingen op het gebied van informatietechnologie, de snelle implementatie en het centraal stellen van IGO door potentiele tegenstanders dwingt de defensieorganisatie ertoe steeds meer de nadruk te leggen op het sneller en slimmer verkrijgen, verwerken, verspreiden en inzetten van informatie. Dit is dus geen keuze, maar absolute noodzaak. De technologie biedt namelijk niet alleen kansen, maar ook dreigingen. Geen gebruik maken van deze technologie betekent met beslissend nadeel opereren. Technologie is echter niet neutraal. Voordat deze wordt toegepast is aandacht nodig voor de mogelijke gevolgen, zeker daar waar inbreuken op grondrechten zoals *privacy* noodzakelijk zijn. Daarbij maakt Defensie onlosmakelijk deel uit van de samenleving. Dit gaat gepaard met meer transparantie richting parlement, partners en publiek en dit stelt hoge (verantwoordings-) eisen aan de omgang met gegevens, informatie en inlichtingen.

IGO is noodzakelijk voor effectief optreden in meerdere domeinen en dimensies tegelijk.

(2) Geopolitieke veranderingen

De wereldorde verandert richting een multipolair stelsel waarin verschillende landen en regio's hun invloed doen gelden buiten multilaterale organisaties als de Verenigde Naties om. Het functioneren van de internationale rechtsorde staat onder druk omdat sommige landen die rechtsorde zien als een Westers construct ten behoeve van Westerse landen.[12] Daarbij neemt de strategische competitie tussen grootmachten toe. Tegelijk proberen opkomende economieën een positie op het wereldtoneel te verwerven waarbij ze zich vaak (nog) niet verbonden hebben aan een grootmacht.

Landen strijden continu om markten, (schaarse) grondstoffen, technologie en de controle over onontgonnen regio's, en zoeken daarbij naar bondgenoten om hun invloed te vergroten. Macht wordt steeds vaker uitgeoefend door de inzet van economische instrumenten, controle over technologieën, uitbuiten van strategische afhankelijkheden en hybride conflictvoering. Informatie speelt hierbij een belangrijke rol. Het vermogen om moderne informatie-technologie zoals kunstmatige intelligentie in het eigen voordeel te benutten draagt in grote mate bij aan onder meer de economische en militaire macht van een land. In deze veranderende geopolitieke context zoekt Europa naar open strategische autonomie.

(3) Veranderende aard van oorlog voeren

Tegelijkertijd gebruiken potentiële tegenstanders verdeel- en heerstactieken om de cohesie binnen de Trans-Atlantische betrekkingen en binnen Europa te verzwakken. Ook proberen potentiële tegenstanders hun strategische doelstellingen te halen zonder de drempel van het gewapend conflict te overschrijden. Het bewust worden van wat er gaande is, deze bewustwording delen met anderen en hier vervolgens duiding aan kunnen geven is van belang om effectief te kunnen reageren op deze potentiële tegenstanders. Tegelijkertijd leert de oorlog om Oekraïne ons dat gevechtsoperaties onverminderd onderdeel blijven uitmaken van oorlog voeren, maar dat het vermogen om te kunnen opereren in de informatieomgeving noodzakelijk is om succesvol te kunnen opereren.

(4) Dreigingen tegen vitale infrastructuur

Vitale handels-, verkeers-, energie- en informatiestromen zijn afhankelijk van infrastructuur. De goede werking van deze infrastructuur, en daarmee alle andere processen die hiervan afhankelijk zijn, kunnen gericht of ongericht bedreigd worden door bijvoorbeeld natuur-geweld, (militaire) sabotage of (geo)politieke instabiliteit. In de bescherming en instand-houding van vitale infrastructuur speelt Defensie, zowel interdepartementaal als internationaal een steeds grotere rol.

[12] De Veiligheidsstrategie voor het Koninkrijk der Nederlanden, 2023

1.4 Samenhang hoofdtaken Defensie

Zoals in artikel 97 van de Grondwet verwoord is, is er een krijgsmacht "ten behoeve van de verdediging en de bescherming van de belangen van ons Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde". De krijgsmacht heeft drie hoofdtaken:

1. Bescherming van het eigen en bondgenootschappelijke grondgebied, inclusief het Caribisch deel van het Koninkrijk.
2. Bescherming en bevordering van de internationale rechtsorde en stabiliteit.
3. Ondersteuning (onder alle omstandigheden) van de civiele autoriteiten bij de handhaving van de openbare orde, de strafrechtelijke handhaving van de rechtsorde, de bestrijding van rampen en incidenten en de beheersing van crises, zowel nationaal als internationaal.

De context is sinds de formulering van deze hoofdtaken wezenlijk veranderd. Er wordt steeds vaker een beroep gedaan op Defensie en de dreigingen zijn toegenomen in aantal, soort en complexiteit. De hoofdtaken raken daarbij meer met elkaar verweven en een helder onderscheid maken tussen de drie is steeds kunstmatiger geworden. Ook wordt steeds vaker onze collectieve meningsvorming bedreigd door grootschalige desinformatiecampagnes. De verdediging en bescherming van ons grondgebied vindt bovendien ver buiten dat eigen grondgebied plaats en overlapt daarmee met de tweede hoofdtaak. De ondersteuning van de civiele autoriteiten bij ordehandhaving, rampen en crises – de derde hoofdtaak – heeft altijd al grote overlap met het beschermen van het eigen grondgebied gehad. We moeten nu en richting 2035 dus zowel dichtbij en binnen ons Koninkrijk als ver weg in het buitenland onze belangen kunnen beschermen.

Het is goed om te beseffen dat de besluitvorming en inzet van militaire capaciteiten niet los kan worden gezien van de andere machtsinstrumenten. Bedreigingen zijn steeds vaker van hybride aard, waardoor de noodzaak tot interdepartementale samenwerking (de geïntegreerde aanpak) toeneemt.

1.5 De geïntegreerde aanpak

Bij een geïntegreerde aanpak worden de machtsmiddelen die een staat ten dienste staan om politiek-strategische doelen te bereiken, op gecoördineerde en samenhangende wijze ingezet, met andere landen en internationale en niet-gouvernementele organisaties. Deze complexe veiligheidsomgeving vereist dat Defensie voor het informatiegestuurd optreden *joint*, inderdepartementaal, multinationaal en met publieke partners (JIMP) moeten kunnen samenwerken.[13] De noodzaak hiertoe stuurt voor een belangrijk deel de eisen die worden gesteld aan het operationaliseren van IGO.

Een goed voorbeeld van de geïntegreerde aanpak is de interdepartementale samenwerking bij het ontwikkelen van een Rijksbreed responskader. In dit responskader wordt een raamwerk neergezet voor het tijdig onderkennen van potentiele (hybride dreigingen) en mogelijke handelingsopties. Hiermee wordt de veerkracht tegen (hybride) dreigingen verder versterkt. Het delen van informatie met andere departementen vergt echter verdere inspanning om gezamenlijk afspraken te maken over de inrichting van de daarvoor benodigde koppelvlakken, rekening houdend met de diverse rollen, taken en verantwoordelijkheden.

[13] Nederlandse Defensie Doctrine, februari 2019.

1.6 Financieel

De in deze beleidsvisie genoemde actielijnen en maatregelen vormen een nadere invulling van de actielijn 6 uit de Defensienota 2022 en zijn financieel gedekt in de begroting en de aanvullende middelen uit de Defensienota 2022 (Kamerstuk 36 124, nr. 1). In de Defensienota 2022 is het CW 3.1 kader opgenomen voor actielijn 6: Informatiegestuurd werken en optreden.

2 Conceptueel kader

2.1 Het domeinmodel en het dimensiemodel

Het militair vermogen van een land wordt niet alleen bepaald door de fysieke slagkracht, maar ook door het moreel van het personeel en door de manier waarop een krijgsmacht operaties uitvoert. Aan die wijze van opereren liggen conceptuele kaders ten grondslag die commandanten helpen de complexe operationele omgeving, waaronder de informatie-omgeving, te kunnen begrijpen en de inzet van het militaire machtsmiddel vorm te kunnen geven. In het Westerse militaire denken is het gemeengoed de operationele omgeving van de krijgsmacht op te delen in domeinen (waarin wordt geopereerd: land, zee, lucht, ruimte en cyber) en dimensies (waarin de te bereiken effecten zich manifesteren: fysiek, virtueel, cognitief).

Domeinen

Het denken in domeinen is instrumenteel om militair vermogen te organiseren voor een specifiek domein. In de moderne oorlogsvoering, en door het toenemende belang en de mogelijkheden van de informatieomgeving, raken de domeinen elkaar steeds meer. Ze vormen een complex geheel van afhankelijkheden en elkaar versterkende processen. Een multidomeinbenadering van de gereedstelling en inzet van militair vermogen is noodzakelijk om geïntegreerde en/of gesynchroniseerde effecten te bewerkstelligen.[14] Het uitschakelen of beschadigen van een zendmast in het landdomein kan bijvoorbeeld voor communicatie-problemen zorgen in de lucht, op zee, in de ruimte, of de toegang tot cyberspace beperken.

[14] Een doel kan onderkend zijn door speciale eenheden op land, waarbij de informatie verstuurd is via een satelliet. Dat doel kan uitgeschakeld worden door gevechtsvliegtuigen, ondersteund met radarbeelden van een fregat terwijl een militaire cyberoperatie de vijandelijke luchtverdediging neutraliseert (NDD)

Dergelijke afhankelijkheden noodzaken ons om het optreden in alle domeinen integraal te benaderen.

Het cyberdomein[15] is een militair domein dat anders is dan de andere domeinen, omdat het een volledig kunstmatig domein is en gedeeltelijk niet-fysiek. Het cyberdomein heeft geen vaste geografische grenzen en strekt zich virtueel uit over de fysieke grenzen van de andere domeinen. Het cyberdomein beperkt zich ook niet in tijd (effecten van een cyberaanval kunnen langjarig effect hebben). Overigens zijn geografische grenzen wel van belang, het gaat om soevereiniteit en nationale verantwoordelijkheden en bevoegdheden. Het cyberdomein kan functioneren dankzij fysieke componenten op land, zee, in de lucht en de ruimte. Omgekeerd zijn operaties in de fysieke domeinen mogelijk door het cyberdomein.
Door op te treden in meerdere domeinen kunnen doelstellingen op een effectievere of efficiëntere manier bereikt worden dan via een enkel domein. Dit pleit voor een multi-domeinbenadering van het militaire optreden.[16] Zo kan bijvoorbeeld een bombardement (luchtdomein) van een rekencentrum een effect bereiken in het cyberdomein. Omgekeerd kan natuurlijk ook, het bewerkstellingen van effecten vanuit het cyberdomein in het land-, lucht-, space-, maritiem of domein.

Dimensies van de informatieomgeving

Het dimensiemodel is een manier van denken om domein-onafhankelijk potentiële effecten en afhankelijkheden van militaire activiteiten binnen de operationele omgeving te duiden. Daarmee zorgt het voor een integrale benadering voor het bereiken van doelstellingen zonder daarbij in de valkuil van een '*single-domain*' benadering te stappen.

Dit dimensiemodel vormt een raamwerk om het doel en de consequenties van militaire activiteiten te kunnen begrijpen, en is daarmee mede bepalend voor de ontwikkeling van effectief militair vermogen. Het raamwerk wordt gevormd door drie dimensies: fysiek, virtueel en cognitief. De te realiseren effecten in deze dimensies zijn uiteindelijk gericht op het (veranderen van) gedrag. In de cognitieve dimensie worden percepties gevormd en besluiten genomen met het oog op de (beïnvloeding van) besluitvorming. Alle dimensies zijn met elkaar verbonden en beïnvloeden elkaar.

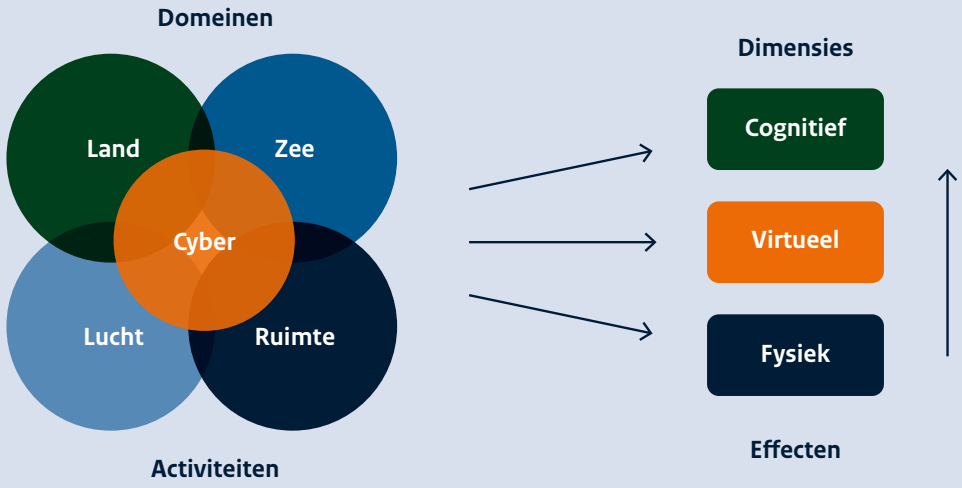
De cognitieve dimensie. Deze dimensie gaat over het beïnvloeden van de wil (emoties, overtuigingen, waarden, percepties, (voor)oordelen, belangen en doelstellingen van individuen en organisaties en omvat alle vormen van onderlinge interactie). Dit is het niet-tastbare deel wat zich afspeelt door het zenden en ontvangen van informatie tussen mensen (sociale laag) en in de hoofden van individuen (cognitieve laag). Hier komt beeldvorming, oordeelsvorming en besluitvorming van actoren tot stand. Dit domein is cruciaal voor het begrijpen en voorkomen of duurzaam oplossen van conflicten.

De virtuele dimensie. Deze dimensie gaat over niet-tastbare communicatie van data, informatie, inlichtingen en kennis zoals tekst en beelden, stuurgegevens, protocollen. Deze niet-tastbare communicatie maakt doorgaans gebruik van cyberspace en het elektromagnetische spectrum. De persona laag is de identificatie van individuen en organisaties in de virtuele dimensie en de logische laag omvat alle bits. Denk aan een e-mailadres, twitterprofiel, avatar, IP-adres, telefoonnummer, etc.

[15] *Cyberspace*: NAVO AJP-3.20 van januari 2020
[16] Nederlandse Defensie Doctrine, februari 2019

De fysieke dimensie. Deze dimensie gaat over alle zichtbare en tastbare elementen die informatie communiceren en/of bij zich dragen, evenals hun geografische locatie, zoals fysieke objecten (satellieten, routers en gebruikersapparatuur, voertuigen en (wapen) platformen), infrastructuur (communicatienetwerken) en de mens als fysiek persoon (als lichaam).

Alle traditionele militaire operatievormen met en tegen fysieke objecten en personen en virtuele objecten zijn bedoeld om (veelal indirect) de wil, perceptie of gedrag van actoren te beïnvloeden. Het geheel van de drie dimensies en de communicatie ertussen biedt meer aangrijpingspunten voor waarneembare en niet-waarneembare, directe en indirecte beïnvloeding. Het brengen van een effect via één van de lagen heeft veelal neveneffecten in andere lagen. Met of tegen elk van de genoemde lagen kunnen (militaire) taken en activiteiten uitgevoerd worden. Uiteindelijk hebben alle activiteiten direct of indirect effect op de cognitieve laag van een doelgroep.



Afbeelding 2.1: **Domeinen en dimensies in relatie tot elkaar**

In het informatietijdperk is het belang van de virtuele dimensie (inclusief benodigde infrastructuur in de fysieke dimensie) enorm toegenomen. Hier wordt onder meer in paragraaf 3.1 verder op ingegaan.

2.2 Informatiemanoeuvre[17]

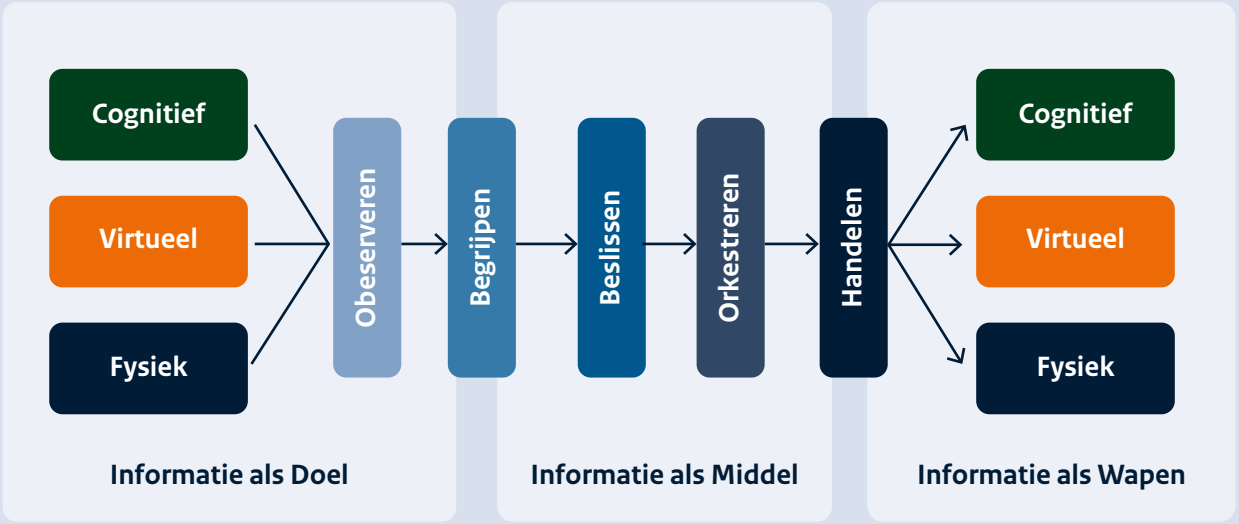
Het gebruik van informatie, in plaats van kinetische effecten, om een opponent te beïnvloeden, noemen we informatiemanoeuvre. Dit is een andere manier van optreden in de informatie-omgeving die, in samenhang met activiteiten in de fysieke dimensie bijdraagt aan het behalen van militaire doelstellingen.

[17] Deze paragraaf is deels ontleend aan het artikel van Peter B M J Pijpers and Paul A L Ducheine, "'If You Have A Hammer': Reshaping the Armed Forces' Discourse on Information Maneuver," ACIL Research Paper 2021-34, 2021. Beschikbaar via: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3954218

Daarmee is Information Manoeuvre een deelaspect van IGO, dat zich vooral richt op het genereren van effecten in de operatieomgeving door het uitvoeren van activiteiten in de informatieomgeving. Deze activiteiten kunnen offensief, defensief of destabiliserend van aard zijn. Hierbij kan worden gedacht aan de inzet van Cybercapaciteiten of Communication & Engagement-capaciteiten, maar ook het beschermen van onze eigen systemen in het elektromagnetisch spectrum of het misleiden van de vijand door ze bewust te confronteren met incomplete of niet-correcte informatie. De inzet van deze capaciteiten komt over het algemeen het beste tot zijn recht als ze in samenhang met de meer traditionele militaire capaciteiten wordt ingezet.

2.3. Samenhang van informatiemanoeuvre en IGO

IGO heeft drie bouwstenen:
Informatie als doel: informatie als bron voor het inlichtingenproces, ten behoeve van *forecasting* (voorspellend vermogen), *insight* (voor beeldvorming), en *foresight* (voor oordeelsvorming), die samen het benodigde begrip van de operatieomgeving opleveren.
Informatie als middel: informatie ter ondersteuning van de commandovoering, voor effectieve besluitvorming en bevelvoering, zowel voor de gereedstelling als de inzet van de krijgsmacht.
Informatie als effector: informatie waarmee effecten in de fysieke, cognitieve en virtuele dimensie kunnen worden bereikt, in een synergetische combinatie met kinetische middelen.



Afbeelding 2.2 **Oorlog in drie dimensies (Bgen P.A.L. Ducheine, NLDA, 2023), afgezet tegen de drie bouwstenen van IGO.**

"Informatie als doel" en "informatie als middel" samen leiden tot het effectiever en efficiënter inzetten van beschikbare capaciteiten . Dit leidt tot mogelijk effecten in alle drie de dimensies, waarbij het uiteindelijk gaat het gedrag van de potentiele tegenstander te beïnvloeden (cognitief) effect. "Informatie als effector" beschrijft zowel het aanpassen van de organisatie

aan de veranderende informatieomgeving als het beter benutten van de mogelijkheden die de virtuele en cognitieve dimensie bieden om onze doelstellingen te realiseren.

Informatiemanoeuvre is het gebruik van informatie om daarmee een gunstige positie te verkrijgen ten opzichte van een opponent. Dat kan op meerdere wijzen vorm krijgen. Hierbij zijn er drie niveaus te onderscheiden:

Niveau 1. Het creëren van een betere informatiepositie dan de opponent. Met de verbeterde informatiepositie kan een beter besluit genomen worden over het inzetten van militaire capaciteiten. De organisatie is hier niet voldoende doorontwikkeld om dit multi-domein of geïntegreerd te doen. Bij de keuze voor de effectoren wordt primair gegrepen naar de bekende (kinetische) middelen (Informatie als doel).

Niveau 2. Hierbij wordt niveau 1 optimaal benut. Daarnaast wordt de commandovoering beter ingericht en beschermd (Informatie als middel). Hierbij is de defensieorganisatie in staat multi-domein en geïntegreerd op te treden op een nader vast te stellen ambitieniveau. Hierdoor wordt sneller data gegenereerd, wordt de interoperabiliteit versterkt en worden effecten beter gesynchroniseerd. Met de beschikking over goede inlichtingen over de tegenstander en diens omgeving, en een optimale commandovoering, kan - op basis van het *targeting* proces - nog steeds worden gekozen voor bekende kinetische effecten (bijv. de wapeninzet van F35s of van het geschut van een fregat) met een duidelijke signaalwerking. Op basis van de inlichtingenpositie en synchronisatie tussen commandocentra, kan een commandant kiezen welk effect het meest geschikt is gegeven de aard en context van het conflict. Deze benadering is een belangrijke aanvulling op het vorige niveau maar nog niet volledig. Daarvoor moet deze benadering ook in samenhang worden bekeken met niveau 3.

Niveau 3. Hier wordt ook gekeken naar andere/nieuwe wijze van optreden en de ontwikkeling van nieuwe *capabilities* die voortkomen uit de ontwikkeling van- en in de informatieomgeving. Dit, in samenhang met niveau 1 en 2 duiden we als informatie-manoeuvre. Hierbij wordt naast de toepassing van “informatie als doel” en “informatie als middel” (optimale commandovoering), de mogelijkheid gecreëerd om naast een kinetisch effect (met signaalwerking) ook effecten in of via de informatieomgeving te sorteren. Dit beïnvloedt de omgevingsperceptie en besluitvormingsmogelijkheden van de opponent met cyberoperaties (1. kinetische effecten) en/of informatie-operaties (2. informatie effecten)

Ad 1. Kinetische effecten: ondermijning en sabotage in de virtuele of fysieke dimensie. Met deze optie wordt getracht elementen in de operationele omgeving aan te passen, te vernietigen, degraderen , neutraliseren, etc. Dit kan op kinetische wijze, zoals het opblazen van een brug of het vernietigen van een radarinstallatie. Maar dit kan ook via de virtuele dimensie, bijvoorbeeld door middel van het aanbrengen van malware zodat een besturings-systeem van de radar of brug niet meer werkt. Als gevolg hiervan kan het radarsysteem of de brug zelfs buiten werking worden gesteld waardoor (indirecte) kinetische effecten ontstaan. De effecten zitten hierbij dus in de virtuele dimensie en in de fysieke dimensie. Essentie is hierbij dat de aanval het doelwit heeft getransformeerd (veranderd, kapotgemaakt etc.).

Ad 2. Informatie effecten: beïnvloeding al dan niet via de virtuele dimensie. Het effect is (zoals overigens alle effecten) direct bedoeld voor de cognitieve dimensie. Gebruikmakend van virtuele identiteiten (bijvoorbeeld sociale media-accounts) wordt geprobeerd mensen te overtuigen – met woord en beeld – hun mening te veranderen, dan wel deze met dwang of manipulatie proberen op te leggen. De beïnvloeding is primair gericht op de wil en attitude (perceptie, wereldbeeld).

Pas op niveau 3 zijn we in staat om informatie ook daadwerkelijk als effector in te zetten om daarmee een informationeel effect te genereren. Op niveaus 1 en 2 genereren we hoofdzakelijk kinetische effecten. Los van de gepresenteerde conceptuele scheiding in deze drie handelingsperspectieven, zal in de praktijk de inzet een combinatie van deze handelingsperspectieven zijn omdat daarmee de meeste synergie wordt bereikt.

De meerwaarde van het concept van informatiemanoeuvre zit in het gebruik van informatie, het beïnvloeden van de informatieomgeving van de opponent en daarmee het beïnvloeden van de perceptie en wil van de opponent. Opponenten passen dit concept ook toe wanneer zij landen in de EU of NAVO aanvallen. De effecten van het aantasten en beïnvloeden worden toegepast zowel binnen als buiten de noties van oorlog en gewapend conflict. De rol die de krijgsmacht kan en moet spelen onder het niveau van gewapend conflict als onderdeel van een geïntegreerde aanpak zal moeten worden uitgevoerd binnen de geldende kaders.

3 IGO: Wat

3.1 Inleiding

De totstandkoming van informatiegestuurd optreden is een transitievraagstuk en vergt een integrale Defensie-aanpak. Het zo veel en zo breed als nodig, rechtmatig, veilig en verantwoord delen en gebruiken van alle relevante data en informatie is daarbij het uitgangspunt. Er is een *roadmap* nodig om investeringen te doen onder meer in IT-infrastructuur en in mensen en manieren om IGO mogelijk te maken. Maar in essentie is IGO is géén programma of project met een begin, een eind, een business case of een budget. Het is een andere manier van denken, organiseren en van werken en kan daarmee worden gezien als *next generation warfare*.

IGO vormt daarmee de basis voor de toekomstige defensieorganisatie. Het verzamelen, snel verwerken en inzetten van betrouwbare informatie, de snellere en betere commandovoering dan de tegenstander, en het aanpassen van het optreden aan de veranderende (mogelijkheden van de) informatieomgeving is in de toekomst vanwege de toegenomen dreiging nog doorslaggevender voor succes.

In deze visie bekijken we IGO langs drie bouwstenen: informatie als doel, middel, en effector. Hieronder zijn de verschillende doelstellingen uit de Defensievisie gekoppeld aan deze bouwstenen. Vervolgens is hetgeen wat met die bouwstenen wordt bedoeld verder uitgewerkt in de paragrafen 3.2 tot en met 3.4.

Informatie als Doel

- We realiseren een goede anticipatiefunctie waarmee we, ter bevordering van de internationale rechtsorde, proactief kunnen optreden in potentiële conflictgebieden en daarmee preventief kunnen opereren
- We hebben inzicht in mogelijke hybride campagnes die zich op verschillende vlakken tegelijkertijd afspelen en kunnen daar met onze partners naar handelen.
- Betrouwbaarheid van informatie (eigen analyse en infopositie) –"gezaghebbende informatiepositie"

Informatie als Middel

- Door een netwerk van commandovoeringselementen kunnen we beter en sneller informatie in samenhang analyseren, filteren en uitwisselen, analyses combineren en zo de gewenste effecten aansturen.
- We hebben betrouwbare, stevige en toekomstbestendige IT en IT-personeel nodig die onze Informatiegestuurde en technologisch hoogwaardige defensieorganisatie ondersteunt en snel aanpasbaar is.
- Multidomein en geïntegreerd denken en optreden is in operaties met nationale en internationale partners het uitgangspunt.
- Onze apparaten, systemen, processen en diensten zijn uitwisselbaar, inpasbaar en samen met partners te gebruiken.

Informatie als Effector

- We versterken ons vermogen om informatieoperaties uit te voeren
- We versterken onze capaciteiten voor elektronische oorlogsvoering
- We versterken de instrumenten voor defensieve en offensieve cyberinzet.

3.2 Informatie als doel

Rijksbreed is er behoefte aan een beter en integraal beeld over de (potentiële) dreigingen tegen het Koninkrijk. Dit betreft interne en externe dreigingen, zowel fysiek als virtueel, tegen de democratische rechtsorde, de territoriale integriteit en soevereiniteit, bevolking, infrastructuur, economie, en overige vitale belangen. Door het tijdig signaleren van potentiële bedreigingen kan escalatie of ontwrichting worden voorkomen. Voor conflictpreventie moet worden geïnvesteerd in het verbeteren van de samenwerking tussen interne en externe veiligheid.[18] Defensie speelt een belangrijke cruciale rol in de interdepartementale aanpak om opkomende conflicten tijdig te onderkennen en daarop in te spelen *early warning/ early action*).

[18] Zie BMH 15 Veiligheid en veranderende machtsverhoudingen, Beleidsvariant E, 20 april 2020, www.rijksoverheid.nl

Door te investeren in "informatie als doel" zijn we als Defensie nog beter in staat doorlopend situationeel beeld en begrip van de omgeving (*situational awareness* en *understanding*) op te bouwen en te behouden over (potentiële) dreigingen in een complexe, hoogtechnologische en informatiedichte omgeving die continue verandert. Door deze informatie te delen met relevante departementen wordt het gezamenlijke beeld van de dreiging versterkt, wat bijdraagt aan een gedeeld beeld.

Vanuit dit gedeelde beeld is het beter mogelijk nationale handelingsperspectieven te ontwikkelen waarmee we de nationale en bondgenootschappelijke veiligheid kunnen vergroten. Defensie kan en moet hierin haar rol nemen in interdepartementaal verband. Dit komt onder andere tot uitdrukking in de Rijksbrede Veiligheidsstrategie en deel strategieën als bijvoorbeeld de Nationale Cybersecurity Strategie.

Defensie streeft ernaar wereldwijd militaire operaties slimmer, sneller en sterker uit te kunnen voeren. Bij slimmer gaat het er vooral om conflicten beter te begrijpen en dat uit te buiten (*to outsmart the enemy*). IGO moet Defensie in staat stellen informatiedominantie[19] te verkrijgen in zowel de fysieke, virtuele en cognitieve dimensie. Hiervoor moet informatie, inclusief inlichtingen op maat, tijdig en op alle niveaus beschikbaar zijn. Dit stelt eisen aan de organisatie en haar processen. Een dominante informatie- en inlichtingenpositie is hiervoor noodzakelijk. Het vermogen om onze omgeving goed te beschrijven (*insight*) en veranderingen aan te zien komen (*foresight*), moet zich continue ontwikkelen en aanpassen aan de veranderende omgeving.

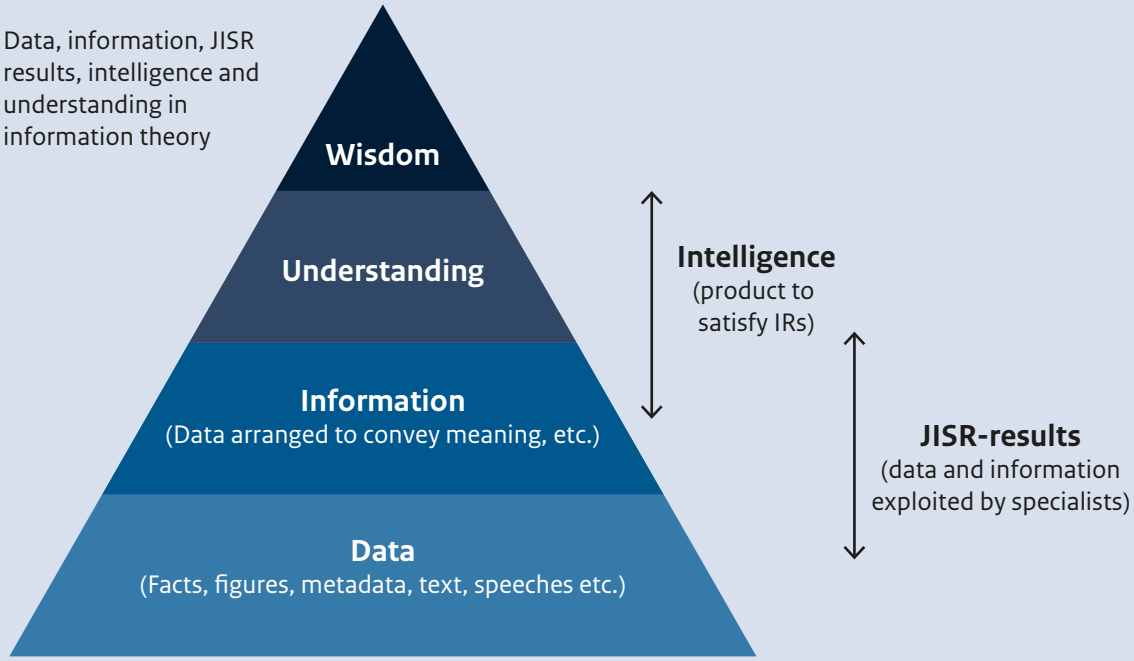
Meer informatie legt echter een steeds grotere druk op de mogelijkheden van het Inlichtingen- en Veiligheidssysteem van Defensie om de besluitvormer van het gewenste omgevingsbeeld te voorzien, ook waar het om de signaalfunctie gaat (*indicators & warnings*). Het is daarom van belang dat op alle niveaus over voldoende capaciteiten wordt beschikt, zodat relevante inlichtingen tijdig beschikbaar zijn voor de commandovoering op alle niveaus (het gestuurd optreden).

Een belangrijk kenmerk van IGO is dat de inlichtingen sneller horizontaal, verticaal en lateraal door de militaire domeinen en organisatie moet kunnen worden verspreid. De complexe, vaak hybride omgeving vraagt om snelle en duidelijke synchronisatie van de beschikbare tijd, het militair vermogen, de gegunde gevechtsruimte en de kwaliteit van de informatie. IGO betekent niet zozeer dat iedereen altijd alle gegevens deelt. Dat hangt immers af van de hoofdtaak, de context van de inzet[20] en de juridische grondslag. IGO betekent dat alle krijgsmachtdelen snel en zorgvuldig met elkaar en met bondgenoten relevante informatie moeten kunnen delen, onder alle omstandigheden, wanneer de inzet dat verlangt.

[19] Informatiedominantie: het initiatief en controle houden over onze operationele omgeving door snel en veilig informatie te kunnen delen tussen de verschillende domeinen en besluitvormingsniveaus om daarmee de dynamische aard van het moderne conflict bij te kunnen benen.

[20] Zie "type operaties", paragraaf 2.4

In het inlichtingenproces worden data en gegevens verzameld om die te ordenen tot informatie en vervolgens te verrijken tot inlichtingen. Zie ook onderstaand figuur[21].



Afbeelding 3.1: Relatie tussen data, informatie en inlichtingen

Vanuit de traditionele benadering bepaalt de wijze waarop de commandant zijn operatie wil uitvoeren, zijn inlichtingenbehoefte. Dat betekent dat het oogmerk en het operatieconcept dat de commandant heeft ontwikkeld (laten ontwikkelen), leidend zijn in de bepaling van de meest cruciale inlichtingen. IGO draait dit paradigma om: de - binnen de juridische en ethische kaders verkregen - beschikbare informatie en inlichtingen (en de verwerking ervan met onder meer *Data Science* en kunstmatige intelligentie) ondersteunen de commandant in het richting geven aan het operatieconcept om zo het gewenste effect te bereiken. In het IGO concept wordt bijvoorbeeld beoogd optimaal effect te bereiken door op basis van informatie de operatie aan te sturen en op de juiste tijd en plaats op de juiste wijze te kunnen optreden. Het IGO proces volgt een cyclus van verzamelen, analyseren van data of gegevens, deze opwerken of veredelen naar informatie, waarbij het doel is vanuit de data te komen tot handelingsperspectief b.v. het optreden of het toepassen van een interventie. In de praktijk komen deze twee werelden steeds meer bij elkaar. Het effect dat een militaire commandant wil bereiken leidt tot een inlichtingenbehoefte. Die bepaalt voor een groot deel de scope van het operatieconcept. Door de beschikbaarheid van grote hoeveelheden data en informatie is een commandant in staat zijn commandovoering verder te verrijken en handelingsopties af te wegen. Dit vergroot de effectiviteit en stelt ons ook in staat om nog meer aandacht te schenken aan andere tweede- en derde orde effecten (bijvoorbeeld nevenschade).

[21] Bron: pagina 92 in de *Allied Joint Publication* (AJP)-2 van de NAVO (versie juli 2020)

Het opbouwen van een informatiepositie en accuraat omgevingsbeeld (*Situational Awareness*) en dit omzetten in handelingsperpectief (*Actionable Knowledge*) is een basisprincipe van IGO. Vervolgens worden de resultaten en uitkomsten als ervaringen vanuit het optreden of de interventie weer meegenomen in de cyclus en dragen ze bij aan het beter begrijpen van dat omgevingsbeeld (*Situational Understanding*) en die kennis te kunnen toepassen (*Wisdom*).
In de steeds complexere omgeving zal iedere dimensie op enige wijze verband houden met de verschillende omgevingsfactoren. Het inlichtingensysteem moet dus in alle dimensies informatie kunnen vergaren om de voor militaire inzet relevante inlichtingen te formuleren.

In vrijwel alle databronnen en informatiestromen die Defensie gebruikt zit wel informatie die betrekking kan hebben op individuele natuurlijke personen. Verwerking van persoonsgegevens dient in overeenstemming met onze Nederlandse en Europese waarden voor vrijheid, democratie en mensenrechten plaats te vinden. In de bedrijfsvoering is dit voor Defensie in beginsel niet anders dan voor andere overheidsinstanties. Denk hierbij aan de personeelsadministratie. Bij de gereedstelling en inzet van de krijgsmacht, moeten we echter uitgaan van bijzondere situaties waarin vitale belangen en mensenlevens op het spel staan. In dergelijke situaties kan het zijn dat privacy onderschikt is aan andere waarden en rechten; zo vereist het oorlogsrecht dat de krijgsmacht in staat is burgers en civiele objecten te onderscheiden om op die manier nevenschade te voorkomen of te minimaliseren. Het is dus van belang om steeds bewust af te wegen binnen welke juridische en ethische kaders de verwerking van persoonsgegevens plaatsvindt en of dat noodzakelijk en proportioneel is. Voordat er sprake is van daadwerkelijk inzet bestaat er echter nog geen grondslag om persoonsgegevens te verwerken, terwijl de krijgsmacht alle systemen wel zo realistisch mogelijk zal moeten kunnen testen en ermee trainen om effectieve en veilige inzet te kunnen garanderen. Hier staat Defensie voor een unieke en complexe opgave. Naast het identificeren en beoordelen van juridische mogelijkheden en beperkingen in verschillende casus, onderzoeken we ook de bruikbaarheid van alternatieven, zoals testen en trainen met geanonimiseerde of synthetische data.

3.3 Informatie als middel

3.3.1 Algemeen

Informatie als middel gaat zowel over gereedstelling als over inzet, maar ook over de ondersteunende en besturende processen die gereedstelling en inzet mogelijk maken. Ondanks dat het vaak gaat over andersoortige data, processen en actoren kunnen ze niet los gezien worden van elkaar, gezamenlijk vormen ze namelijk de waardeketen van Defensie . Effectieve inzet is alleen mogelijk door de adequate combinatie van politiek-ambtelijke besturing en militaire commandovoering, vervulling van personele en materiële behoeften, gereedstelling en ondersteuning. Deze primaire en ondersteunende hoofdprocessen dienen integraal te worden geoptimaliseerd met inzichten uit data en toepassing van technologie omdat het invulling geven aan alle drie de hoofdtaken gebeurd vanuit dezelfde set aan militaire capaciteiten (*single set of forces*). Hierbij heeft inzet en gereedstelling van capaciteiten voor de ene taak altijd gevolgen voor de gereedstelling en inzet van een andere taak. Bij digitale transformaties spreekt men vaak over het drieluik mensen, manieren en middelen (*people, process, en technology*[22]). De wijze waarop de gereedstelling, inzet, ondersteuning en besturing/commandovoering is vormgegeven is onlosmakelijk verbonden met de algehele

[22] Zie ook https://www.forbes.com/sites/brentdykes/2021/06/01/10-reasons-why-your-organization-still-isnt-data-driven/?sh=5ab24f2c7d80 Hier staat vermeld dat de grootste uitdaging voor het worden van een data-gedreven organisatie niet de technologie is (7,8%) maar ligt bij de mensen, processen en culturele aspecten (92.2%)

effectiviteit van Defensie. Door gebruik te maken van de hedendaagse technologische mogelijkheden als *Data Science* en AI, kunnen we zowel in de bedrijfsvoering al tijdens gereedstelling en inzet slimmer, sneller en beter werken.

3.3.2 Gereedstelling

De operationele gereedheid van de krijgsmacht bestaat uit de personele gereedheid, de materiele gereedheid en de geoefendheid. De analyse van wat daar voor nodig is, wordt jaarlijks vastgelegd in de Aanschrijving Gereedstelling Defensie (AGDEF). Hier ligt ook een relatie met het proces Strategie en Krijgsmacht Ontwikkeling (SKMO). Dit is een proces dat ervoor moet zorgen dat de doelen, manieren en beschikbare middelen (*ends, ways & means*) altijd met elkaar in balans ziin.Dit is een arbeidsintensief proces waarvoor veel gegevens nodig zijn. Toepassingen van *data science* en AI kunnen deze processen en besluitvorming ondersteunen door sneller beter inzicht te geven in de gereedheid en plannen van de krijgsmacht in de tijd.

3.3.3 Operationele processen

De NAVO hanteert het concept van geïntegreerd multidomeinoptreden in een hybride context waarin statelijke tegenstanders al hun Diplomatieke, Informatie, Militaire en Economische (DIME) machtsinstrumenten gebruiken om hun strategische doelen te bereiken. Daarbij maken ze optimaal en ongelimiteerd gebruik van nieuwe technologieën. Hiermee hebben zij de mogelijkheid om de OODA[23]-loop sneller te doorlopen dan wij, wat hen sterk in het voordeel brengt.

Multi Domein Optreden (MDO)

Multi-domeinoptreden vindt zijn oorsprong in de Verenigde Staten. Een aantal militaire analisten zag een dergelijke wijze van optreden tijdens de Russische annexatie van de Krim en de gevechts-handelingen in Oekraïne. Rusland had een grondige analyse gemaakt van de succesvolle *AirLand Battle* doctrine en het *Follow-on Forces Attack* concept van de VS en had hierin de zwakke punten had gevonden. Dit speelde zich af toen de VS zich met name bezighield met het herontdekken van *counterinsurgency*. Door een sterke focus op militaire inzet in het kader van vredesmissies (Hoofdtaak 2, Wars of Choice) had het Westen al jaren geen zicht meer op een conflict met een gelijkwaardige tegenstander, zoals we nu zien in Oekraïne. De conceptuele en technologische ontwikkeling in Rusland richtte zich met name op het tegengaan van westers lucht- en maritiem overwicht. Dit resulteerde in de zogenaamde A2/AD, *Anti-Access/Area Denial*: het voorkomen dat een tegenstander zijn strijdkrachten kan inzetten in een bepaald gebied door de toegang te ontzeggen middels gekoppelde radarsystemen, superieure raketsystemen, lange-dracht artillerie en EOV stoor- & opsporingscapaciteit. China hanteert op dit moment een soortgelijke A2/AD-strategie in onder meer de Zuid-Chinese Zee, teneinde de toegang tot China te voorkomen.

Waar in het verleden de nadruk lag op de synchronisatie van activiteiten en effecten in de verschillende domeinen tijdens het gevecht, is het in de huidige context van belang nog voorafgaand aan een gewapend conflict in een goed uitgangspositie te komen wanneer er

[23] OODA: Observe - Orient - Decide - Act

nog handelingsopties bestaan om escalatie te voorkomen. Daarbij vereist multidomein optreden ook de verdere integratie met de activiteiten van andere departementen en civiele partners om daarmee succesvol op te kunnen optreden tegen de nieuwe dreigingen. Dit vergt niet alleen aandacht voor de afweging welke informatie voor wie beschikbaar moet zijn, maar ook een andere mentaliteit: van *need to know* naar *need to share*. Uit oogpunt van operationele veiligheid of nationale belangen kan het nodig zijn een deel van de informatie af te schermen.[24]

Een voorwaarde voor een effectieve, efficiënte en geïntegreerde inzet van militair vermogen is het kunnen toepassen van "informatie als middel" voor snelle en effectieve besluitvorming. Dit vereist dat effectenbrengers, sensoren, commandovoeringselementen in verschillende en wisselende samenstelling veilig gegevens en informatie kunnen uitwisselen met behulp van moderne communicatie- en informatiesystemen. Deze interconnectiviteit maakt grotere interoperabiliteit mogelijk: Nederlandse eenheden kunnen geïntegreerd optreden met bondgenootschappelijke strijdkrachten, al naar gelang de situatie in verschillende en wisselende, ofwel gefedereerde, samenstellingen. Dit vermogen om militaire capaciteiten naadloos met elkaar te verbinden en te laten samenwerken in gefedereerde verbanden, staat binnen de NAVO bekend als *Network Enabled Capabilities*.

De huidige verregaande digitalisering introduceert het risico van informatie-overload[25]. Om de operationele processen te ondersteunen is een expliciete afweging over de voor- en nadelen van additionele gegevens vooraf noodzakelijk daarnaast is goede verwerkings- en analysecapaciteit van belang om tijdig bruikbare informatie op het gewenste niveau te brengen. Adequaat informatiemanagement is cruciaal om informatie op het juiste moment op de juiste plaats beschikbaar te hebben waarmee optimale en snellere beslissingen kunnen worden genomen. IGO is daarmee een *force multiplier*.

De toegenomen mogelijkheden in digitalisering leiden tot een groter aanbod aan zeer diverse informatiebronnen (waarvan het merendeel *open source* is), die een belangrijke aanvulling kunnen zijn op de door eigen of bondgenootschappelijke verworven informatie. Deze aanvulling stelt ons in staat de informatiekwaliteit en –snelheid te vergroten ten gunste van besluitvorming en bevelvoering. Al deze data opent nieuwe mogelijkheden en nieuwe inzichten maar kent ook risico's en is begrensd door wet- en regelving[26]. Niet alles wat technisch kan, mag en is wenselijk. Dat vraagt om complexe afwegingen; zo moeten we het grondrecht op privacy afwegen tegen andere belangen.; dat is een continu proces op alle niveaus: bij het maken van beleid en regelgeving, bij het ontwerpen van informatiesystemen, bij het verlenen van mandaten voor een missie, en bij het nemen van militair-tactische beslissingen. Het zoeken naar de juiste balans tussen kunnen, willen en mogen is hierbij van belang.

Het verbeteren van IGO is echter niet alleen een technisch vraagstuk. Ook procesmatige, personele, culturele en organisatorische aspecten spelen hier een belangrijke rol. Het is juist de samenhang van al deze aspecten die snelle en gerichte informatiestromen mogelijk maakt, om daarmee een grotere snelheid van handelen en besluitvorming te krijgen dan die van de tegenstander. Het zijn dus niet alleen technische netwerken, maar ook sociale netwerken die van groot belang zijn. Met sociale netwerken leveren de noodzakelijke menselijke maat, belangrijk voor het creëren van vertrouwen. Een goed voorbeeld hiervan is de inzet van

[24] Nederlandse Defensie Doctrine, 2019
[25] Dit geldt niet alleen overigens niet alleen voor "informatie als middel" maar ook voor "informatie als doel".
[26] Onderzoekscommissie Land Information Manoeuvre Centre, "Grondslag gezocht", december 2022.

liaisonpersoneel en van personeel op multinationale hoofdkwartieren. Direct persoonlijk contact zal nooit volledig kunnen worden vervangen door de uitwisseling van digitale beelden, geluiden en teksten.

3.3.4 Ondersteuning

Om de randvoorwaarden voor gereedstelling en inzet te scheppen, zijn ondersteunende processen nodig van cruciaal belang: als eerste het vervullen van de personele behoefte met het werven en opleiden van personeel en het vervullen van de materiële behoefte door de verwerving van materieel, inclusief IT en vastgoed. Vervolgens het tijdens de gereedstelling of de inzet leveren van ondersteuning aan de operationele eenheid onder meer in de vorm van aanvullende opleidingen voor personeel, militaire gezondheidszorg, specialistisch hoger onderhoud aan materieel, onderhoud aan vastgoed en IT- infrastructuur, logistieke en facilitaire ondersteuning en informatie en inlichtingenvoorziening. Met het inzetten en verder ontwikkelen van technologie en (voorspellende) inzichten uit data kunnen ondersteunde processen beter aansluiten bij de voor de gereedstelling en inzet benodigde capaciteiten en het op niveau houden van deze *capaciteiten*. Voorbeelden zijn toepassing van *Predictive Maintenance* en intelligent vraag- en aanbod management.

3.3.5 Besturing

Besturen in de context van Defensie omvat het bepalen van de missie (in relatie tot de grondwettelijke taken), actief vooruitkijken voor de ontwikkeling van de krijgsmacht, organiseren, leidinggeven, coördineren, monitoring en regie en het afleggen van verantwoording . Binnen het concept van informatiegestuurd optreden is het noodzakelijk dat deze taken en gerelateerde processen eveneens verregaand geoptimaliseerd worden met behulp van inzichten uit data-analyse en de inzet van technologie. Het verzamelen, analyseren en koppelen van data (en/of informatie) uit verschillende bedrijfsvoerings-systemen, voor zover dat is toegestaan binnen de juridische kaders, biedt inzicht en handelingsperspectieven om werving, verwerving, opleiden en trainen maar ook op het gebied van financiën, logistiek en het onderhoud van materieel, gebouwen en terreinen te verbeteren en waar nodig te versnellen. Op die manier kan IGO bijdragen aan een optimale werking van het Beleid-, Plannen en Begrotingsproces (BPB) en daarmee het realisatie- en transformatievermogen en het lerend vermogen van Defensie.

3.4 Informatie als effector

3.4.1 Algemeen

Beïnvloeding van tegenstanders door in te spelen op hun informatiepositie is van alle tijden, of dat nu het verstoren van radars is of het bewust misleiden door valse informatie over een aanstaande aanval te verspreiden. In de informatieomgeving kunnen op verschillende wijzen effecten worden gesorteerd. In de informatieomgeving kan daarbij onderscheid worden gemaakt tussen drie dimensies: de tastbare fysieke dimensie, de niet-tastbare cognitieve dimensie (de wil, perceptie en gedrag van een individu) en virtuele dimensie (de enen en nullen, maar ook sociale media accounts).

De potentie van informatie als effector is enorm toegenomen door technologische ontwikkelingen. We zien bijvoorbeeld dat mensen via het internet dagelijks worden beïnvloed, maar ook welke rol het internet speelt bij de verspreiding van informatie rondom conflicten. Enerzijds is de afhankelijkheid van informatie voor militaire en niet-militaire toepassingen toegenomen. Het gaat daarbij om toepassingen van alledaagse aard, maar ook om toepas-singen van vitale en strategische aard. Anderzijds is de beschikbaarheid van informatie en informatie-verwerkende systemen toegenomen.

Bij het hanteren van informatie als effector, ofwel gebruik van informatie om de tegenstanden te beïnvloeden kan onderscheid worden gemaakt in Cyberoperaties, Elektromagnetische activiteiten (of in combinatie als CEMA) en Informatie-operaties.

3.4.2 Cyberoperaties

Het cyberdomein biedt mogelijkheden aan de krijgsmacht, maar evengoed aan tegenstanders. De krijgsmacht moet dus enerzijds kunnen optreden tegen tegenstanders in *cyberspace* en anderzijds de eigen operaties kunnen ondersteunen en beschermen; en dat terwijl de technische mogelijkheden blijven toenemen in aantal en complexiteit. Door sterk onderling verbonden en nauw geïntegreerde netwerken en systemen, is de krijgsmacht kwetsbaar voor risico's, zoals verminderde betrouwbaarheid of beperkte bruikbaarheid van netwerken en systemen. De vrijheid van handelen in alle domeinen is daarmee afhankelijk van de cyberveiligheid en –weerbaarheid en de vrijheid van handelen die we hebben in het elektromagnetisch spectrum.

Cyberoperaties[27] zijn initieel gericht tegen (de bedienaars van) digitale systemen, netwerken of apparaten van de tegenstander. Dit gaat om sensor-, wapen- en C2-systemen, (personele en materiële) logistieke ketens, (militaire) vitale infrastructuur en het brede scala aan losse apparaten die zijn verbonden met het internet. Voor een goede werking is ieder digitaal object afhankelijk van juiste en tijdig beschikbare informatie. Het initiële effect wordt altijd in de 'logische laag' gecreëerd, zoals software, operating systems, applicaties en andere datacomponenten (de nullen en enen). De manipulatie van objecten in de logische laag veroorzaken ander gedrag van objecten in de fysieke laag. Een voorbeeld hiervan is het toenemend gebruik van *ransomware*, waarbij de data van partijen wordt gegijzeld en de dreiging van sabotage, namelijk het permanent verwijderen van deze data, een waardevolle criminele businesscase is geworden.

Cyberspace staat evenwel ook indirect in verbinding met de cognitieve dimensie, waarbinnen doelwitten kunnen worden geselecteerd en aangegrepen. Effecten in de virtuele dimensie kunnen indirecte effecten (2e en 3e orde) in elk van de overige dimensies veroorzaken en daarmee uiteindelijk de perceptie, wil en gedrag van een gewenste doelgroep mensen beïnvloeden. Denk hierbij aan *hack-and-leak* operaties of aan desinformatie campagnes. Op die manier kunnen cyberoperaties een ondersteunende rol spelen bij informatieoperaties (de term die hier steeds vaker voor gebruikt wordt is *cyber enabled* operaties.) Cyberspace kan fungeren als platform (de vector) waarmee de informatie gerelateerde middelen of methoden (zoals strategische communicatie, informatie-operaties of psychologische oorlogvoering) worden overgedragen, maar ook om vergelijkbare (informatie)operaties van een tegenstander tegen te gaan.

Het cyberdomein is de digitale weerspiegeling van de fysieke componenten binnen het land-, lucht-, maritieme en ruimtedomein. Vrijheid van handelen in alle domeinen is daarmee te beïnvloeden via cyberspace. Cyberspace kent weliswaar fysieke elementen in andere domeinen (zoals computers, servers, netwerken), maar het bereik van haar effecten wordt nauwelijks beïnvloed door bestaande grenzen of gebruikelijke fysieke beperkingen van andere domeinen. Het mondiale en alomvattende karakter van *cyberspace* biedt daarnaast toegang tot een breed palet aan mogelijke doelen: variërend van strategisch en operationeel tot tactisch. Kritische randvoorwaarde hiervoor is het hebben van de juiste inlichtingenpositie om deze effecten te kunnen bereiken. Cyberoperaties kunnen autonoom worden uitgevoerd, of in combinatie met andere (militaire) operaties. Daar waar effecten worden uitgebracht die

[27] Als cyberspace objecten, activiteiten of instrumenten als militair middel worden ingezet voorbij de soevereine grenzen van het domein van de eigen staat, dan is het internationale recht van toepassing.

zijn gericht op digitaal verbonden netwerken die voor hun verbindingen ook gebruik maken van het EMS ligt afstemming tussen het optreden in cyberspace en het EMS voor de hand. Deze specifieke vorm van afgestemd optreden in het elektromagnetisch spectrum en cyberspace wordt CEMA[28] (*Cyber Electromagnetic Activities*) genoemd.

3.4.3 Informatie-operaties

Cyberoperaties beogen primair een effect in cyberspace (Cyber-identiteit laag, Logische laag en Fysieke laag), wat (in)direct effecten kan sorteren in de fysieke en cognitieve dimensie. Informatie operaties beogen primair een effect in de cognitieve dimensie. In het laatste geval is de informatie het effector en kan de cyberoperatie faciliterend, de 'wapendrager', zijn. Uiteraard hebben effecten in de virtuele en fysieke dimensies ook hun weerslag in de cognitieve dimensie. Een ander verschil wordt bepaald door de omvang van de operationele omgeving. Waar cyberoperaties alleen plaatsvinden in, of via cyberspace, kunnen informatie-operaties plaatsvinden in iedere omgeving.

Om uiteindelijk effectief te zijn, zowel offensief als defensief, zijn inlichtingen cruciaal. De link met "informatie als doel" is evident.

Voor strategische communicatie in de complexe informatieomgeving is eenduidige en duidelijke communicatie gekoppeld aan politieke- of militaire doelstellingen cruciaal. Het inrichten van een centrale strategische communicatiefunctie binnen Defensie, naar voorbeeld van de NAVO, die de strategische communicatie van de krijgsmacht in beeld, woord en daad synchroniseert en daarin samenwerkt met andere departementen en internationale samenwerkingsverbanden, zoals EU en/of NAVO is daarvoor een voorwaarde.

Volgens de NAVO Joint doctrine zijn psychologische operaties geplande activiteiten die gebruik maken van communicatiemethodes en andere middelen gericht op een vooraf gedefinieerd publiek om percepties, houding en gedrag te beïnvloeden om zo politieke en militaire doelstellingen te bereiken. De traditionele flyer in een operatiegebied is hier een voorbeeld van. (AJP-3.10.1)

Deceptie is een combinatie van middelen om een tegenstander te misleiden door het manipuleren, vernietigen of vervalsen van feiten zodat hij reageert op een manier die ingaat tegen zijn eigen belang. Dit kan gedaan worden door zijn perceptie van de feiten te veranderen of zijn gedrag te beïnvloeden zodat dit voordeel oplevert voor ons. (AJP 3-10.2)

Communication and Engagement (C&E): Het beter begrijpen en beïnvloeden van gedrag van mensen, (sociale) netwerken, online informatieverspreiding en -consumptie en de dynamiek van de achterliggende narratieven. Dit leidt tot beter inzicht en begrip van een situatie of doelgroep.

Cyber enabled C&E. Met Cyber enabled C&E wordt het beïnvloeden van de perceptie en het gedrag van mensen via de virtuele dimensie bedoeld: het cyberdomein is hier de aanvals-vector. Te denken valt aan berichten op sociale media om doelgroepen (burgers, combattanten, etc) te overtuigen of hun gedrag en gedachtes te manipuleren of beïnvloeden.

[28] Het elektromagnetisch spectrum (EMS) omvat verscheidene types van elektromagnetische straling, variërend van radiogolven tot zichtbaar licht en gammastraling. Vanuit een militair oogpunt kan het EMS als drager (brenger) van informatie op een directe manier worden benut. Ook kan het EMS indirect worden gebruikt, bijvoorbeeld voor het creëren van effecten (jamming, spoofing of gerichte energie-wapensystemen). De relatie tussen cyberspace en de elektromagnetische activiteiten (EMA) is eerder complementair dan competitief. Dit komt met name door de digitalisatie van Electronic Warfare en het gebruik van het EMS; beide voorheen vooral analoog.

Dit om uiteindelijk een gewenst effect te bereiken zoals een goed beeld van de NAVO-interventie of een slechter beeld van een tegenstander.

Door bovenstaande inzichten kunnen effectievere interventies worden ontwikkeld om het eigen narratief beter over te brengen, om *hearts & minds* te winnen, om burgers te beschermen of om opponenten/agressoren effectiever aan te grijpen.

4 Richtlijnen voor het hoe

4.1 Inleiding

Deze beleidsvisie spitst zich toe op de vragen 'Wat is Informatie Gestuurd Optreden?' en 'Waarom is een fundamentele IGO-transformatie van onze defensieorganisatie noodzakelijk?' Daarmee geeft dit document generieke sturing voor de ontwikkeling van Defensie richting de ambities zoals neergezet in de Defensienota 2022. In dit hoofdstuk worden de randvoorwaarden en de actielijnen voor de verdere operationalisering van IGO beschreven.

4.2 Randvoorwaarden voor het operationaliseren van IGO

Hieronder worden een aantal randvoorwaarden benoemd, die bij de verdere uitwerking en concretisering van deze visie van belang zijn.

Juridische en ethische kaders
Kunnen, willen en mogen; om gezien de continue en snel veranderende dreigingen de grondwettelijke taken van de krijgsmacht uit te kunnen blijven voeren, zal Defensie samen met belanghebbende partijen (zowel binnen als buiten Defensie) voortdurend moeten blijven verkennen en testen hoe er binnen de bestaande juridische en ethische kaders effectief gehandeld kan en mag worden. Hiervoor is steeds integrale afstemming tussen verschillende professionele groepen in de organisatie nodig, zoals militairen, juristen, beleidsmakers, privacy-experts en beveiligingsfunctionarissen. Experimenteren met informatiegestuurd optreden vraagt een goede en nauwgezette beoordeling en begeleiding van de risico's binnen de kaders van het *Concept Development & Experimentation* (CD&E) beleid.

Hybride conflictvoering en nieuwe dreigingen raken aan de kern van waar de Krijgsmacht voor staat, vastgelegd in de Grondwet en beleidsmatig uitgewerkt in drie hoofdtaken. Bij informatiegestuurd optreden kan het verwerken van persoonsgegevens nodig zijn. De mandaten die binnen en buiten de defensieorganisatie afgegeven kunnen en mogen worden

om met gegevens en informatie te werken zijn een randvoorwaarde om informatiegestuurd op te treden.[29] Als in specifieke situaties blijkt dat de krijgsmacht taken niet kan uitvoeren vanwege juridische beperkingen, zal ook bezien of de wet- en regelgeving herijkt moeten worden. Om een wettelijke grondslag voor de verwerking van s te bieden is democratische, parlementaire besluitvorming nodig. Een dergelijke herbezinning op de beleidsmatige en juridische kaderstelling waarbinnen de krijgsmacht opereert, is fundamenteel en omvangrijk en moet zorgvuldig worden onderbouwd.

Robuustheid en weerbaarheid

Defensie dient haar eigen informatie- en wapensystemen tegen cyberaanvallen te beschermen (*cyber resiliency*). Dit maakt deel uit van haar eigen digitale weerbaarheid. Daarnaast dient Defensie redundantie (back-up systemen) in te bouwen voor informatie- en wapensystemen; hieronder valt ook informatie *resiliency*: de mate van redundantie waarin informatie via verschillende wegen tot je kan komen (fysieke dimensie, informatiedragers). Ook zal Defensie nauw samen moeten werken met de aanbieders van vitale processen en aan de bescherming daarvan moeten (kunnen) bijdragen in geval van een (cyber)conflict.

IGO data ontsluiting, connectiviteit en interoperabiliteit bij grote projecten

De koppeling tussen IGO en grote materieelprojecten spitst zich toe op de kernvraag: "In hoeverre houdt Defensie bij de verwerving van groot materieel – en breder gezien bij het ontwikkelen van capaciteiten – rekening met IGO?" Aspecten die daarbij van belang zijn, zijn onder andere principes als *privacy en security by design* en *default*, zeggenschap over gegevens, interoperabiliteit, connectiviteit, *data-labeling* en filtering, dataverzameling en –ontsluiting en cybersecurity. Hierbij geldt dat het niet alleen moet gaan om het platform zelf, maar ook om de (informatie)omgeving waarin dat platform moet opereren. Daarom moeten zowel IT als wapensysteem programma's' voldoen aan de architectuureisen voor de informatiegestuurde krijgsmacht.

Samenwerken

De ontwikkelingen op het gebied van IGO gaan razendsnel, waardoor Defensie niet in alle gevallen in staat is om alles zelf te doen. Meer dan ooit kijkt Defensie naar kennisinstellingen, industrie, NAVO/EU partners voor samenwerking en het benutten van reeds ontwikkelde oplossingen. Zowel de Strategische Kennis en Innovatie Agenda[30] als de Defensie Industrie Strategie[31] zetten in op een weloverwegen balans tussen het volgen van civiele ontwikkelingen en het ontwikkelingen van militaire toepassingen in samenwerking met onze private partners.

Datamanagement en *data governance*[32]

Om de kwaliteit van gegevens te waarborgen, standaarden vast te stellen, en juist gebruik van gegeven te waarborgen is data governance en gegevensbeheerder noodzakelijk. De defensie-onderdelen kennen ieder hun eigen dynamiek en behoeven hun eigen aanpak om invulling te geven aan het Informatiegestuurd optreden met behulp van data. Er is echter een aantal gemeenschappelijke uitdagingen die om een integrale aanpak vragen: geschikte technologische voorzieningen, inzicht in de manier waarop data science en AI impact zullen hebben op de werkzaamheden en vaardigheden van onze medewerkers en data management en governance. Naast technologische mogelijkheden, is een goed uitgewerkte, breed gedragen

[29] Zie ook: Algemene juridische kaders voor activiteiten van de krijgsmacht in de informatie-omgeving (12 April 2021, Bijlage bij Kamerbrief van 7 mei)
[30] Strategische Kennis- en Innovatieagenda (SKIA) 2021-2025, november 2020
[31] Defensie Industrie Strategie (DIS), november 2018
[32] Zie ook Defensie Strategie Data Science en AI.

en ingerichte data governance een belangrijke randvoorwaarde voor het behalen van onze ambities. Defensie heeft de taken, verantwoordelijkheden en bevoegdheden op dit vlak vastgelegd en werkt momenteel aan de professionalisering hiervan.

Security by design[33]
Bij de ontwikkeling van data science en AI-toepassingen is beveiliging een integraal en belangrijk onderdeel van het ontwerpproces moeten zijn (security-by-design principe) om kwetsbaarheden in de systemen te voorkomen. Daarbij dient rekening gehouden te worden met databeveiliging en rubricering waarbij het koppelen van systemen voor bepaalde toepassingen nieuwe vraagstukken met zich mee brengt. Omdat er veel verschillende systemen en situaties voorkomen in een militaire context, beoordelen we dit per geval.

Privacy by design
Wet- en regelgeving stelt specifieke eisen aan de verwerking van persoonsgegevens zodat het grondrecht van privacy wordt beschermd. Volgens de Algemene Verordening Gegevensbescherming (AVG) moet de verwerking van persoonsgegevens voldoen aan beginselen van:
- Rechtmatig, zorgvuldig en transparant
- Doelbinding (welbepaald, uitdrukkelijk omschreven en gerechtvaardigd)
- Minimale gegevensverwerking
- Juistheid
- Opslagbeperking
- Integriteit en vertrouwelijkheid (passende technische en organisatorische maatregelen)
- Verantwoordingsplicht

Bij ontwerp is toepassing van *Privacy by design* verplicht en geldt dat voor hoge *privacy* risico's voorafgaand een Data Privacy Impact Assessment (DPIA) wordt opgesteld. Een DPIA is bedoeld om *privacy* risico's in kaart te brengen en draagt bij aan het vermijden of verminderen van deze risico's.

4.3 Actielijnen voor het operationaliseren van de beleidsvisie IGO

Naast het feit dat deze beleidsvisie een gemeenschappelijke (conceptuele) basis biedt voor het actualiseren van (deel)strategieën en andere beleidsproducten, is deze visie tevens de basis voor het verder concretiseren van IGO en het ontwikkelen van de hiervoor benodigde capaciteiten. Dit gebeurt langs zes actielijnen.

Actielijn 1: Commandovoeringsprocessen en –structuren.
Om optimaal gebruik te kunnen maken van de mogelijkheden die de digitale transformatie biedt, zal ook de manier waarop Defensie haar civiele besturing heeft ingericht en met de militaire commandovoering heeft verweven aangepast worden. Het moderne conflict vereist een mate van flexibiliteit en adaptiviteit die hiërarchische besluitvormingsstructuren niet kunnen bieden, omdat die langzamer werken. Een plattere netwerkstructuur op alle niveaus van oorlogvoering (strategisch, operationeel en tactisch) heeft in een dynamische omgeving een beter zelf-orkestrerend vermogen omdat het zich kan aanpassen aan de verschillende contexten in de operationele omgeving, waarbij het uitgangspunt is dat verantwoordelijkheid daar in het netwerk wordt belegd waar de beste *situational understanding* is. Het uitgangspunt daarbij is opdrachtgerichte commandovoering, waarbij bevoegdheden naar het laagst mogelijke niveau zijn gemandateerd. Daarnaast zal de commandovoering opnieuw ingericht

[33] Zie ook Defensie Strategie Data Science en AI.

moeten worden volgens een te ontwikkelen Multidomein Optreden (MDO) Concept, waarbij de commandovoeringselementen informatie uit alle domeinen ter beschikking hebben en deze kunnen verwerken naar opdrachten die synergetische effecten geven in de verschillende domeinen. Een eerste noodzakelijke stap die zal worden gezet is het inrichten van een Operationeel Hoofdkwartier, dat verantwoordelijk is voor multidomein commandovoering op het operationele niveau.

Actielijn 2: Het (fysieke en sociale) netwerk dat sensoren, verwerkings- en analysecapaciteit, commandovoeringselementen en effectoren met elkaar verbindt en de effectoren aanpast aan de veranderingen in de informatieomgeving.
Om de complexe uitdagingen van moderne oorlogvoering het hoofd te kunnen bieden, en daarnaast optimaal gebruik te maken van de mogelijkheden van de digitale transformatie, is een herziening van de manier waarop de diverse entiteiten binnen onze organisatie met elkaar verbonden zijn en samenwerken noodzakelijk. De operationele context waarin wij opereren is veranderlijk; binnen korte tijd moeten we kunnen schakelen tussen optreden in een Hoofdtaak 1 scenario naar ondersteuning van nationale partners in een Hoofdtaak 3 scenario, of in een context waarin de Hoofdtaken in elkaar overlopen. Al deze mogelijke inzetopties vragen om een ander samenstel van sensoren, verwerkings- en analysecapaciteit, commandovoeringselementen en effectoren en een goed inzicht in juridische en ethische kaders. De mogelijkheden voor informatiemanoeuvre die ontstaan door de ontsluiting van de informatieomgeving voor militair optreden versterken deze noodzaak tot verandering. Om optimaal gebruik te maken van de kansen in de informatieomgeving, en voorbereid te zijn op digitale bedreigingen, zal Defensie ook in dit nieuwe domein een gedegen netwerk van sensoren tot en met effectoren (cyberoperaties, EMS operaties en informatieoperaties) moeten creëren om daarmee effectief te zijn in alle dimensies. Deze elementen moeten gekoppeld kunnen worden aan de elementen in de klassieke domeinen zodat er in samenhang gestreefd kan worden naar synergie. Defensie moet in staat zijn om haar middelen en manier van werken snel en vloeiend aan te passen aan de veranderende context. Hiertoe is een federatief missienetwerk nodig waarbij vooraf is nagedacht over filtering en *data labeling*. Hierin kunnen verschillende elementen (sensor, commandovoering, informatie, effector) in verschillende domeinen aan elkaar worden gekoppeld naar gelang de aard van de situatie. Deze federatieve structuur creëert flexibiliteit en adaptiviteit. Daarnaast mitigeert een federatief netwerk de kwetsbaarheden van een klassiek hiërarchisch en gecentraliseerd systeem, waarbij het uitschakelen of verstoren van een enkele schakel, bijv. een cyberaanval op een hoofdkwartier, de gehele operatie kan platleggen. Dit moeten we ook kunnen beoefenen.

Actielijn 3: De mentaliteit en de manier van werken.
IGO is een manier van denken en werken die tot in de haarvaten van de organisatie door moet dringen. Door de huidige technische en organisatorische beperkingen op het delen van informatie zit het '*need-to-know*' principe nog diep verweven in de manier van denken en doen van het personeel. De toevoeging van informatiemanoeuvre aan de militaire gereedschapskist noodzaakt fundamentele aanpassingen aan de manier van het plannen, voorbereiden en uitvoeren van operaties. De conceptuele benadering van informatie als effector zal integraal onderdeel uit moeten gaan maken van onze operationele processen.
Deze factoren noodzaken een verandering van de mentaliteit van Defensiemedewerkers die uiteindelijk leidt tot cultuurverandering in de gehele organisatie. Dit vraagt om interventies in verschillende aandachtsgebieden, zoals werving, opleiding en training maar ook leiderschap. Het is van belang dat het leiderschap van Defensie, op alle niveaus, doordrongen is van het belang van deze verandering en deze ook actief uitdraagt. Dit kan bijvoorbeeld ingevuld worden door het organiseren van masterclasses. Daarnaast dient IGO in de curricula van

initiële en loopbaanopleidingen worden opgenomen. Deze opleidingen dienen aandacht te besteden aan competenties die de werknemers in staat stellen effectief te opereren in de veranderende context. Ook zal Defensie haar oriëntatie op de arbeidsmarkt moeten aanpassen om personeel met geschikte eerder verworden competenties te werven.
Ook betekent deze verandering dat er meer aandacht moet worden besteed aan juridische en ethische kaders. Naast het optimaal benutten van bestaande wet- en regelgeving is het ook van belang structurele oplossingen op het gebied van wet- en regelgeving verder te verkennen.

Actielijn 4: Een robuuste en veilige IT-infratructuur als fundament voor IGO.
Hoewel IGO veel meer omvat dan de technische component, is een robuuste en veilige IT-infrastructuur inclusief IT-organisatie een noodzakelijke voorwaarde voor het slagen van de IGO-transformatie. Het federatieve netwerk van actielijn 3 heeft een federatief IT-fundament nodig om effectief te zijn. Dit IT-fundament moet voorzien in een aantal randvoorwaarden die het mogelijk maken om multi-domein en op alle niveaus van oorlogvoering tijdig en veilig over de juiste informatie te kunnen beschikken. Onze huidige IT-infrastructuur wordt vernieuwd middels programma's als GrIT. Hierdoor wordt het mogelijk om snel, geautoriseerd en veilig gegevens en informatie te kunnen delen tussen de verschillende eenheden en besluitvormingsniveaus, zodat we in staat zijn om de dynamische aard van het moderne conflict bij te benen.

Een aantal aandachtspunten zijn daarbij van bijzonder belang. Ten eerste moet de IT-infrastructuur informatie en inlichtingen wereldwijd kunnen ontsluiten in zowel de statische als de ontplooide, mobiele en uitgestegen omgeving. Daarnaast zal dit veilig moeten gebeuren, met koppelingen tussen de verschillende rubriceringsniveaus zodat personeel over alle informatie kan beschikken waar zij conform hun rol en veiligheids-machtiging toegang toe hebben. Verder dient de IT-infrastructuur bestand te zijn tegen verstoringen van technische aard of door acties van een externe actor.

Actielijn 5: Onze connectiviteit en interoperabiliteit met bondgenoten en partners.
In veruit de meeste gevallen zal Nederland niet alleen opereren, maar in bondgenoot-schappelijk verband, gelegenheidsverbanden (coalitions of the willing), of met nationale partners in het veiligheidsdomein. De connectiviteit – oftewel het technisch kunnen koppelen met anderen – en de interoperabiliteit –het werken volgens gelijke standaarden en afspraken– moet daarom in al onze wapensystemen, netwerken en processen ingebakken zitten.
In bondgenootschappelijk verband betekent dit dat Defensie in staat is om met informatie als doel, middel en effector te kunnen samenwerken. Dit vraagt in de eerste plaats dat het nationale beleid aansluit op bondgenootschappelijke doctrine en concepten. Het uitgangs-punt is "NAVO tenzij" wat ertoe moet leiden dat Defensie met dezelfde standaarden werkt om snel en efficiënt met bondgenoten data en informatie te kunnen uitwisselen.
In het nationale veiligheidsdomein betekent dit dat Defensie en nationale veiligheidspartners in staat moeten zijn bij nationale inzet geautomatiseerd informatie uit te wisselen om een gedeeld beeld en gezamenlijk begrip van de veiligheidssituatie te kunnen opbouwen teneinde samenwerking met publieke partners te optimaliseren, uiteraard binnen de vigerende juridische en ethische kaders.

Actielijn 6: Informatiegestuurd gereedstellen, ondersteunen en besturen.
Informatiegestuurd optreden is alleen effectief als ook de overige hoofdprocessen uit de waardeketen van Defensie (gereedstellen, ondersteunen en besturen) optimaal gebruik maken van inzichten uit data en informatie. Een toename in het gebruik van data en informatie zorgt voor een betere informatiepositie. Bestuurders op alle niveaus krijgen beter inzicht en zijn daardoor beter in staat om te anticiperen op veranderende omstandigheden.

Op het gebied van ondersteuning betekent dat het inzichtelijk maken en verkorten van doorlooptijden in de aanvoerketen. Daarnaast zorgt het gebruik van data en informatie voor een betere aansluiting van ondersteuningsprocessen bij de inzet en gereedstelling en inzet van de krijgsmacht. Om de hoofdprocessen besturing en ondersteuning verregaand te kunnen ondersteunen met inzichten uit data en informatie is het noodzakelijk dat aan een aantal voorwaarden wordt voldaan. Deze voorwaarden zijn te categoriseren rondom de volgende aandachtsgebieden: organisatie (o.a. capaciteiten, werkwijze, cultuur), processen, data & informatie en technologie.

Colofon

Locatie	Den Haag - Plein-Kalvermarktcomplex Kalvermarkt 32 ‘s-Gravenhage
Postadres	Postbus 20701 2500 ES ‘S-GRAVENHAGE MPC 58B
Versie	VERSIE 1.3 d.d. 30 juni 2023

Ministerie van Defensie
Juli 2023